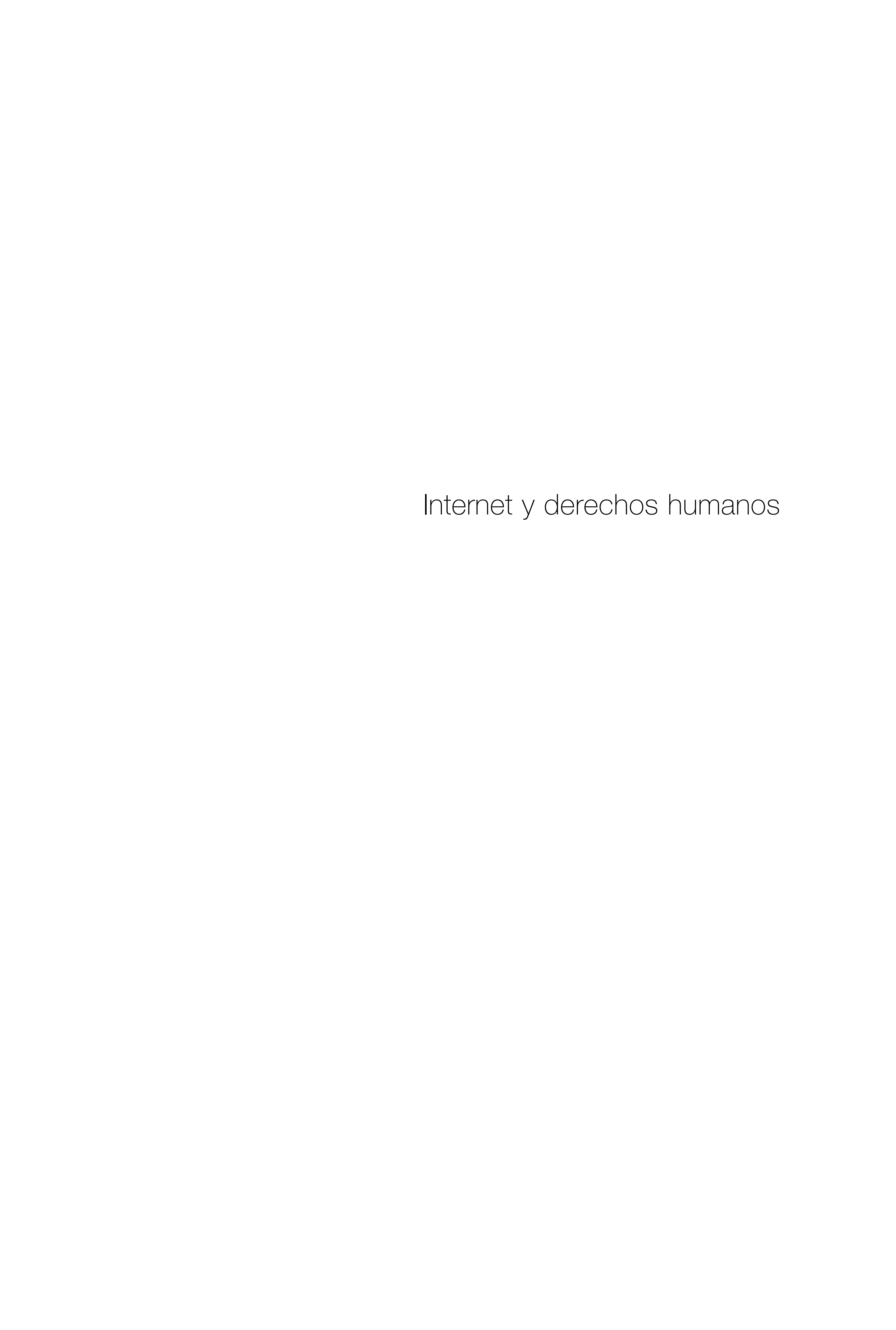
Internet y derechos humanos
Aportes para la discusión en América Latina

Eduardo Bertoni
COMPILADOR

Facultad de Derecho
Centro de Estudios en Libertad de
Expresión y Acceso a la Información







Internet y derechos humanos

Internet y derechos humanos

Aportes para la discusión en América Latina

Eduardo Bertoni

COMPILADOR


Facultad de Derecho

Centro de Estudios en Libertad de
Expresión y Acceso a la Información





Cortés Castillo, Carlos
Internet y derechos humanos : aportes para la discusión en América Latina / Carlos Cortés Castillo y Eduardo Andrés Bertoni ; compilado por Eduardo Andrés Bertoni.
- 1a ed. - Ciudad Autónoma de Buenos Aires : Del Puerto, 2014.
176 p. ; 23x15 cm.

ISBN 978-987-3671-01-2

1. Derechos Humanos. 2. . 3. Políticas Públicas. I. Bertoni, Eduardo Andrés II. Bertoni, Eduardo Andrés, comp. III. Título
CDD 320.6

Fecha de catalogación: 09/01/2014

Compilador
Eduardo Bertoni

Diseño gráfico y diseño original de tapa:
Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo

Editado por el CELE, febrero de 2014, Buenos Aires, Argentina.

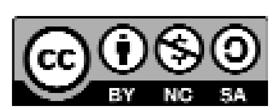
ISBN: 978-987-3671-01-2

Hecho el depósito que marca la ley 11.723

Esta edición, de 200 ejemplares, se terminó de imprimir en el mes de febrero de 2014 en Voros S.A. Bucarelli 1163. CABA

Impreso en la Argentina
Printed in Argentina

Mario Bravo 1050 (C1175ABW)
Ciudad de Buenos Aires. Argentina
Tel.: (54 11) 5199-4500
Fax: (54 11) 4963-1560
cele@palermo.edu |
www.palermo.edu/cele



Esta compilación de artículos de la Iniciativa por la Libertad de Expresión en Internet del CELE se publica gracias al apoyo financiero de Global Partners Digital en el marco del proyecto Global Internet Freedom Project.

Índice

Introducción

Eduardo Bertoni

¿Cómo debería regularse Internet desde una perspectiva de derechos humanos?

Esta pregunta es muy amplia y encierra algunas cuestiones que parecen saldadas, aunque no es tan así. La primera cuestión que la pregunta asume como respondida es que es necesario regular Internet. Sobre este particular han existido muchos debates. Sin embargo, el fiel de la balanza parece estar inclinándose en favor de la existencia de algún tipo de intervención del Estado en temas vinculados con Internet.

Asumida la necesidad de la regulación, el interrogante gira hacia los límites que debería tener esa regulación. Y allí es donde una persepectiva desde los derechos humanos aparece como relevante.

El Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo, desde sus inicios, ha buscado, con sus trabajos, esbozar posibles respuestas a la pregunta inicial. En ese marco, en 2012, el CELE lanzó la Iniciativa por la Libertad de Expresión en Internet (iLEI)[1], un programa especial que tiene como objetivo proporcionar asesoramiento y apoyo técnico a los promotores y hacedores de políticas en materia de Internet.

Neutralidad de la red, privacidad, derechos de autor, responsabilidad de intermediarios y su relación con los derechos fundamentales son algunas de

---

[1] El iLEI es dirigido por Eduardo Bertoni. En la iniciativa han participado Carlos Cortés Castillo, como Investigador Principal, y Verónica Ferrari, Atilio Grimani y Daniela Schnidrig como asistentes de investigación.

las cuestiones que ha abordado el iLEI en sus trabajos. Hemos considerado que estos temas son los que más se han tratado en las regulaciones y propuestas legislativas que se empezaron a elaborar en América Latina en los últimos años.

El primero de los artículos que aquí presentamos, *La neutralidad de la red: la tensión entre la no discriminación y la gestión,* comienza con una breve explicación de la arquitectura de la red, a partir de los principios que sustentan la idea de neutralidad. Más adelante, examina la definición de neutralidad de la red y los problemas que enfrenta cuando se plantea su implementación. El artículo señala, entre otras cosas, que las excepciones a la neutralidad de la red deben establecerse en conjunción con la obligación de no discriminación dado que categorías como «gestión razonable» pueden desvirtuar la garantía de neutralidad. Además, el artículo explica los argumentos en contra de este principio.

Este trabajo, que da un vistazo a la legislación en Europa y América Latina, da cuenta de la necesidad de regular el principio a través de una ley aprobada por el Congreso ya que, solo así, se garantiza un debate amplio y adecuado sobre las características y el alcance de una regulación en la materia. Asimismo, señala que la implementación de las normas sobre neutralidad de la red merece tanta atención como la elaboración de los marcos regulatorios.

El artículo que sigue, *Vigilancia en la red: ¿qué significa monitorear y detectar contenidos en Internet?,* se detiene en el interés, cada vez mayor, por parte de los gobiernos de monitorear la red. El artículo analiza el concepto de control en Internet, haciendo énfasis en el rol de los intermediarios y en el uso de tecnologías como la Inspección Profunda de Paquetes. Asimismo, plantea la tensión entre la seguridad nacional y la prevención de la violencia, y derechos fundamentales como la libertad de expresión y la privacidad.

La conclusión de este documento es que el monitoreo de los contenidos en línea pone en riesgo las garantías fundamentales de los ciudadanos y amenaza el entorno digital abierto y pluralista que conocemos hasta hoy. Por esto, este trabajo del iLEI recomienda delimitar y transparentar el uso que hacen los gobiernos de las herramientas de monitoreo y vigilancia de Internet. Asimismo, señala que los proyectos de ley y las iniciativas regulatorias que buscan establecer mecanismos de monitoreo de contenidos en Internet deberían contar, previamente, con estudios técnicos de impacto en derechos humanos.

Las llaves del ama de llaves: la estrategia de los intermediarios en Internet y el impacto en el entorno digital, el artículo siguiente, retoma algunas

cuestiones esbozadas en el trabajo anterior y profundiza lo relacionado con la teoría de los guardianes (o amos de llaves) en Internet.

Este artículo, en primer lugar, explora las teorías generales de los intermediarios y su relación con la responsabilidad civil. Más adelante, analiza el balance entre los costos que asumen los intermediarios y los beneficios que obtienen por hacer de guardianes. El artículo señala que un desequilibrio entre estos costos y beneficios implica «una estrategia fallida que además impacta negativamente en actividades socialmente deseables y afecta derechos fundamentales como el debido proceso y la libertad de expresión».

El artículo da cuenta de los antecedentes que llevaron a los intermediarios de Internet a asumir este rol de guardianes de los usuarios y explora los tipos de intermediarios que existen, cuáles son sus deberes y los modelos de responsabilidad que les caben. Hacia el final, este trabajo advierte sobre el riesgo de pensar al filtrado de contenidos como una alternativa para el problema de la responsabilidad de los intermediarios y propone explorar soluciones tecnológicas para equilibrar el debate en Internet.

Más adelante, se presentan dos trabajos en materia de derechos de autor y las tensiones con el ejercicio de la libertad de expresión y el acceso a la cultura en el entorno digital. El primero de ellos, *La tensión entre la protección de la propiedad intelectual y el intercambio de contenidos en la red,* parte del caso del sitio argentino Cuevana y el proyecto denominado «ley Lleras» en Colombia como puntos de partida para analizar posibles colisiones entre la excesiva protección de los derechos autorales y el intercambio de contenidos a través de Internet.

En líneas generales, el documento señala que la protección de los derechos de autor en detrimento de derechos elementales, como el debido proceso y la libertad de expresión, obliga a preguntarse cuál es realmente la prioridad de los Estados en cuanto a gobernanza de Internet. Además, sostiene que, como pasó en Colombia con las sucesivas «leyes Lleras», la presión internacional y las obligaciones contraídas en tratados internacionales hacen pensar que América Latina va camino a adoptar leyes excesivamente restrictivas en la materia.

El otro artículo, *Libertad de expresión versus libertad de expresión: la protección del derecho de autor como una tensión interna,* encara una discusión teórica que no ha sido suficientemente abordada. En general, se habla de las tensiones entre los derechos de los autores y la libertad de expresión de los usuarios de Internet. Este documento sostiene, en cambio, que el copyright también es un desarrollo de la libertad de expresión. El artículo, entonces, pro-

pone examinar los proyectos y las leyes sobre propiedad intelectual a partir de esta «tensión interna» entre dos formas de expresión y sostiene que es necesario hacerlo sin preconceptos de cuál es la protección más importante.

En *Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital* se abordan los debates actuales en torno a la creación de un nuevo derecho al olvido que le devuelva al individuo el control sobre su información y lo libre de su «pasado digital».

Este trabajo del iLEI ofrece un panorama general del tema: esboza una definición de derecho al olvido y su posible tensión con otros derechos existentes, y plantea su vínculo con la protección de datos o hábeas data. Hacia el final, el artículo brinda algunas propuestas para introducir una especie de olvido en el entorno digital y señala que, a la hora de buscar soluciones, se debería contemplar a todos los actores involucrados en Internet, empezando por los usuarios.

Por último, el artículo *Nombres de dominio: una expresión que merece ser protegida. Recomendaciones y sugerencias para administradores locales de América Latina y el mundo* aborda la relación entre libertad de expresión, los nombres de los dominios y los distintos modelos que adoptan los países para administrarlos. Este trabajo parte de la idea de que los nombres de dominio son una forma de expresión y opinión y, por ende, los administradores de registro y renovación deberían tener en cuenta los estándares internacionales que garantizan los derechos de opinión y expresión.

En esta línea, en sus recomendaciones el trabajo señala que los Estados deberían contar con administradores independientes de la injerencia gubernamental. Por ello, señala el documento, los modelos en los que participan múltiples sectores interesados pueden ser un ejemplo a seguir.

Sin perjuicio de los aportes y recomendaciones que hacemos en los artículos antes reseñados, creemos que un buen principio para discutir políticas en materia de Internet en América Latina, basadas en principios de derechos humanos, surgen de una Declaración Conjunta sobre Libertad de Expresión e Internet[2] emitida por los relatores especiales de Naciones Unidas, la OEA, la Organización para la Seguridad y la Cooperación en Europa y la Comisión Africana de Derechos Humanos y de los Pueblos. Los relatores en materia de libertad de expresión, en este documento publicado en 2011, señalan lineamientos que deberían tenerse en cuenta a la hora de regular Internet. Por ejem-

2 http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&.

plo, hablan de la necesidad de que no se trasladen mecánicamente modelos que se aplican a los medios tradicionales. Si bien es cierto que Internet comparte ciertas características con estas tecnologías, también es cierto que es muy distinta en otros aspectos como en materia de alcance global, (bajos) costos, y la posibilidad de que la utilicen un número ilimitado de usuarios. Entonces, afirman los relatores, normas que no han sido específicamente pensadas para Internet pueden afectar de manera negativa el ejercicio de derechos clave. La declaración, asimismo, hace referencia a cuestiones específicas vinculadas al límite al bloqueo y filtrado de contenidos, a la importancia de la neutralidad de la red, a la responsabilidad de los intermediarios y a la necesidad de elaborar políticas públicas en materia de acceso universal.

Finalmente, queremos destacar que esta publicación ha sido realizada gracias al apoyo financiero de Global Partners Digital en el marco de un proyecto en conjunto con el CELE que se ha desarrollado en 2013 y 2014. El libro reúne los trabajos del iLEI desde su creación y tiene como objetivo principal servir de insumo para los debates de políticas públicas y proyectos legislativos que se discuten en la actualidad.

Buenos Aires, febrero de 2014
Iniciativa por la Libertad de Expresión en Internet (iLEI)
del Centro de Estudios en Libertad de Expresión
y Acceso a la Información (CELE),
Facultad de Derecho, Universidad de Palermo.

La neutralidad de la red: la tensión entre la no discriminación y la gestión[1]

Resumen

El objetivo de este documento es examinar el concepto de neutralidad de la red con la idea de identificar los puntos clave de la definición y los problemas que enfrenta cuando se plantea su implementación.

En la primera parte se hace una explicación breve de la arquitectura de la red, a partir de los principios que sustentan la idea de neutralidad: modularidad, estratificación y extremo a extremo. En seguida se describe el inicio del debate en Estados Unidos. Fue allí donde la neutralidad de la red surgió asociada a la obligación de transporte común o *common carrier.* En tercer lugar, se explican los argumentos en contra de la neutralidad y algo sobre la práctica. Aunque la mayoría de éstos suelen catalogarse como justificaciones comerciales, tiene relevancia en la conceptualización misma de la neutralidad. Más adelante, se da un vistazo a la legislación en Europa y América. Según lo

---

[1] Este documento fue elaborado por Carlos Cortés Castillo, investigador de la Iniciativa por la Libertad de Expresión en Internet (iLEI), del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo. La investigación y elaboración del documento fue dirigida y contó con los comentarios de Eduardo Bertoni, director del CELE. Carlos Cortés Castillo es abogado de la Universidad de Los Andes, Colombia, con maestría en Gobernanza de Medios del London School of Economics, Reino Unido. Fue director de la Fundación para la Libertad de Prensa (FLIP) y profesor de Derecho de Medios del Programa de Periodismo y Opinión Pública de la Universidad del Rosario, Colombia. Actualmente es asesor de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos y del Programa de Medios de Open Society Foundations, en temas relacionados con regulación de Internet y libertad de expresión. Ha trabajado como periodista en medios de comunicación colombianos como *Semana* y *La Silla Vacía*.

que allí se describe, el nudo gordiano está en las excepciones a los deberes de no discriminación y gestión razonable de la red. Por último, se ofrecen algunas conclusiones y se hacen las siguientes recomendaciones:

• La regulación sobre neutralidad de la red debe estar contenida en una ley expedida por los congresos de los Estados. Solo así se garantiza un debate adecuado y amplio sobre las características y el alcance de una ley en la materia.

• Las excepciones a la neutralidad de la red deben establecerse en conjunción con la obligación de no discriminación. De lo contrario, bajo categorías como la «gestión razonable» se termina desvirtuando la garantía de neutralidad.

• La idea de reconocer los servicios especializados ofrecidos por los prestadores del servicio de Internet como algo distinto al Internet abierto puede a la postre fortalecer el concepto de neutralidad de la red. Propuestas como la de la Coalición Dinámica por la Neutralidad de la Red deben ser parte de las discusiones en materia de política pública.

• Relacionado con lo anterior, la posibilidad de que existan paralelamente servicios preferenciales y el Internet abierto no puede, de ninguna manera, desembocar en la degradación de esta última.

• La implementación de las normas sobre neutralidad de la red merecen tanta atención como su diseño. Debe trabajarse en la documentación de casos y en la labor de monitoreo del gobierno.

• Los principios sobre neutralidad de la red parecen perder vigencia en el ámbito de los servicios móviles. Teniendo en cuenta que el acceso a Internet va moviéndose paulatinamente a las plataformas móviles, es importante que el trabajo de la sociedad civil y de los reguladores se centre también en este aspecto.

I. Introducción

Para quienes siguen los debates sobre la regulación de Internet, difícilmente existe un término más trillado que el de «neutralidad de la red». Suele brillar en todas las discusiones y entre más se usa menos claro queda su significado. Pareciera que sucede lo mismo que con la palabra «censura» en materia de libertad de expresión: significa algo diferente en cada contexto.

La idea de neutralidad de la red, sin embargo, ha recorrido un breve pero intenso camino desde que fuera formulada por el estadounidense Tim Wu en 2003. De ser un planteamiento académico pasó a ganar importancia en las discusiones sobre política pública. Hoy implica una serie de principios que ya

están plasmados en varias leyes. Hoy por hoy podemos decir que la neutralidad de la red existe.

¿Existe en teoría? ¿Existe en la práctica? No hay duda de que la arquitectura original de Internet incorporó unos principios de diseño que dan sentido a la idea de neutralidad. Pero tampoco hay duda de que en el desarrollo y expansión de la red éstos se han ido desconociendo y están en tránsito de modificarse. La neutralidad es un territorio en disputa.

El objetivo de este documento es examinar el concepto de neutralidad de la red con la idea de identificar los puntos clave de la definición y los problemas que enfrenta cuando se plantea su implementación.

El texto se desarrolla de la siguiente manera, primero, se hace una explicación breve de la arquitectura de la red; segundo, se sitúa la idea de neutralidad en el contexto del debate norteamericano, donde surgió; tercero, se explica el caso contra la neutralidad de la red y se describe algo sobre la práctica; cuarto, se da un vistazo a la legislación, y quinto, se ofrecen algunas conclusiones y recomendaciones.

II. Arquitectura de Internet y neutralidad de la red

Internet fue creado siguiendo tres principios de diseño: el de modularidad, el de estratificación y el de extremo a extremo. Estos principios determinan «la manera como un sistema se descompone en sus componentes, cómo la funcionalidad se distribuye a través de esos componentes, o cómo los componentes dependen unos de otros».[2] A continuación se explica cada uno.

II.A. Modularidad

La arquitectura de un sistema difiere en relación a si sus componentes están acoplados estrechamente o de manera laxa. En esa medida, el principio de modularidad dispone que los componentes sean altamente independientes, o sea, que no estén demasiado acoplados. Esto permite que el sistema se pueda dividir en varios módulos con interdependencias mínimas, lo cual no quiere decir que no haya relación entre éstos; los puntos de interacción de los módulos existen, pero se limitan únicamente a lo necesario y están definidos en la

[2] Van Schewick, B., *Internet Architecture and Innovation*, The MIT Press, Cambridge, Massachusetts, 2010, pos. 446 (versión Kindle). Traducción informal. La explicación de este capítulo se basa en este libro.

etapa de diseño de la arquitectura (la relación entre los módulos no puede modificarse en etapas posteriores).

El propósito de la modularidad es que los componentes puedan diseñarse de manera independiente y descentralizada y aun así funcionar juntos. Las computadoras personales son el mejor ejemplo. La interfaz entre los dispositivos periféricos –impresora, pantalla, ratón– y el resto del sistema está previamente especificada, y se ocupa únicamente de definir las características del conector y el tipo de datos que debe transmitir. A partir de allí, los diseñadores están en absoluta libertad para crear su dispositivo.

El principio contrario al de modularidad es el de integridad, según el cual hay interdependencias entre todos los componentes, con lo cual cada decisión sobre el diseño debe estar acorde con todas las partes de la cadena. Los productos de Apple siguen ese principio. «El resultado en términos de diseño puede ser más eficiente o tener un rendimiento global mayor que el del sistema modular», explica Van Schewick.[3]

II.B. Estratificación

Si bien la modularidad establece que la interdependencia entre los componentes debe ser mínima y estar previamente definida, no dice nada sobre la manera en que interactúan los módulos entre sí. Para este fin, en Internet este principio se complementa con el de estratificación o capas, que restringe las interacciones entre los módulos. «El uso de las capas permite asignar funciones separadas y encadenadas de una a otra: cada capa sirve a la de más arriba y ésta, a su vez, sirve a la siguiente. Usualmente, la capa superior cumple una función más compleja que la anterior».[4]

Las computadoras, los sistemas operativos y las aplicaciones hacen parte de una arquitectura estratificada. Así, el disco duro, el monitor y la impresora están en el nivel más bajo; el sistema operativo, en la capa superior, y las aplicaciones, en la de más arriba. Cada capa conoce únicamente la información de la capa que le sigue, y no necesita más que eso para funcionar. Así, quien desarrolla una aplicación solo necesita saber en qué sistema operativo va a funcionar su programa (técnicamente, su aplicación debe ser compatible con la interfaz de programación de aplicaciones del sistema operativo) y, a partir de

---

3 *Ibídem*, pos. 557.

4 Op. cit, Cortés Castillo, p. 6.

allí, puede crear un producto. De la misma manera, quien desarrolla un sistema operativo solo necesita conocer la interacción con el equipo donde éste va a operar.

La arquitectura de Internet está compuesta, en términos generales, por cuatro capas que permiten dividir las funciones de la red. Para llevar a cabo su misión, cada capa usa los servicios de la que le precede. La capa más baja es la de «enlace», que contiene los protocolos responsable del transporte de paquetes a través de una red física (por ejemplo, la de una oficina o universidad); le sigue la capa internet, que permite transportar paquetes a través de un conjunto de redes interconectadas, sin importar en dónde esté cada dispositivo; en seguida, está la capa de transporte, que reparte los paquetes desde y hacia las aplicaciones de los dispositivos finales; por último, está la capa de aplicaciones, que contiene una serie de protocolos que permiten la comunicación entre las partes (correo electrónico, *world wide web*, redes de pares, video).

El hecho de que haya capas permite que cada nivel trabaje y se desarrolle sin preocuparse por lo que pasa en los demás niveles, salvo por el que le antecede. Igualmente, la estratificación incrementa las posibilidades de cambios en el sistema, ya que las modificaciones en las capas superiores no afectan a las capas inferiores.

II.C. Extremo a extremo

Por último, el principio de extremo a extremo sirve para decidir qué función debe cumplir cada capa en el sistema, y propone que entre más específicas sean las funciones, más arriba deben estar situadas. Esto implica que las funciones que solo sean necesarias para una aplicación en particular deben estar en la capa más alta (y más cercana al usuario), mientras que aquellas que son generales para el sistema deben ubicarse en las más bajas.

Esta ilustración del principio es vertical –del tubo de la calle, pasando por la computadora de la casa, hasta el correo electrónico que enviamos–. Pero su aplicación también es horizontal: las funciones más elaboradas de la red deben estar en los extremos, es decir, en los dispositivos que se conectan a la red y no en los enrutadores o computadoras del medio que transmiten los datos. Es por esta razón que el principio de extremo a extremo suele describirse como el de un una red «tonta» (*dumb network*) con inteligencia en los extremos.[5]

---

[5] Cfr. Marsden, C., *Net Neutrality. Towards a Co-regulatory Solution*, Bloomsbury Academic, Londres y Nueva York, 2010.

El propósito de este principio, en su sentido horizontal, es que la red sea lo menos especializada posible y se dedique simplemente a «servir» a los extremos para que estos funcionen de todas las formas imaginables.[6] Es decir, para que los extremos puedan innovar –un propósito que subyace también a los principios de estratificación y modularidad–.

Estos tres principios se complementan con el método que emplea Internet para transmitir los datos, conocido como la «conmutación de paquetes de datos» o *packet switching.* La conmutación de paquetes implica que todos los datos –sin importar su contenido o características– se parcelan en el punto de origen y se transmiten por la red en cualquier orden y por rutas distintas hasta llegar al destino final. Solo allí se rearman en su estado original y se vuelven asequibles para el usuario.

Cada paquete contiene una parte de los datos enviados e información sobre el destino y las instrucciones para rearmarse allí (mediante los protocolos TCP/IP). Lo único que la red debe hacer –a través de los enrutadores– es transportar esos paquetes; éstos contienen la demás información. No obstante, los protocolos del envío de paquetes no garantizan un resultado; se trata de un sistema de «mejor esfuerzo».[7] Si en el camino un paquete se pierde, habrá que intentar de nuevo. El efecto para el usuario es que, por ejemplo, la página de Google no carga, el video de YouTube se retrasa o la llamada de Skype se cae.[8]

Son estos principios los que apuntalan la idea de la neutralidad de la red. En palabras de Lawrence Lessig, «una consecuencia de este diseño, entonces, es que la gente puede innovar para esta red sin necesidad de coordinar con alguno de sus propietarios».[9] La arquitectura de la red hace que bajen los costos para desarrollar nuevos servicios y, sobre todo, evita que los propietarios de los tubos y cables actúen estratégicamente a favor de uno u otro contenido.

---

[6] Cfr. Wu, Tim, *The Master Switch: The Rise and Fall of Information Empires*, Vintage, Random House, 2010.

[7] Cfr. Wu, Tim, «Network Neutrality, Broadband Discrimination», *Journal of Telecommunications and High Technology Law,* Vol. 2, p. 141, 2003, disponible en: http://ssrn.com/abstract=388863 (consultada el 13 de octubre de 2013).

[8] Para una explicación más detallada sobre el *packet switching*, ver op. cit. Cortés.

[9] Lessig, L., *Code 2.0,* Basic Books, Nueva York, 2006, p. 111.

III. De Estados Unidos para el mundo

Aunque el término «neutralidad de la red» (*network neutrality*) fue acuñado por el académico norteamericano Tim Wu en 2003,[10] no se trataba de un concepto del todo nuevo. La idea de neutralidad venía antecedida por los conceptos de «acceso abierto» y «transporte común» (*common carrier*), usados en los sectores de telecomunicaciones y transporte en las décadas previas. De la misma forma, Wu no era el primero en hablar del tema. Para entonces académicos como Lawrence Lessig, Mark Lemley y Kevin Werbach, sin referirse a «neutralidad», ya estaban escribiendo sobre los desafíos del Internet abierto.[11]

Sin entrar aún en una descripción detallada, las primeras definiciones de neutralidad de la red en Estados Unidos apuntaban a una regla simple: todo el contenido en Internet debe moverse igual y a la misma velocidad a través de la red. Internet no debe favorecer ninguna aplicación por encima de otra. En estos términos, la neutralidad comprende dos compromisos de no discriminación de parte de los prestadores del servicio de Internet: uno de servicio universal y otro de transporte común (*common carriage*).[12]

El punto inicial del debate se dio por cuenta de las posibles integraciones entre los Proveedores del Servicio de Internet (PSI) y las compañías de cable.[13] Es decir, era una discusión sobre competencia y monopolios. El temor principal consistía en que si los operadores de cable podían empaquetar la oferta de servicios de televisión con la de acceso a Internet, terminarían por excluir aplicaciones o servicios que les compitieran.

Y es que el impacto de los monopolios en las telecomunicaciones y el entretenimiento en Estados Unidos o, más bien, la manera como los monopolios han moldeado estos sectores, aparece en el espejo retrovisor de la historia de Internet. Quizá el caso más célebre fue el del AT&T, que se integró

---

[10] Cfr. Wu, *supra* nota 7.

[11] Cfr. Marsden, *supra* nota 5.

[12] Cfr. Brown, I. y Marsden, C., *Regulating Code. Good Governance and Better Regulation In the Information Age,* The MIT Press, Cambridge, Massachusetts, 2013.

[13] En Estados Unidos las compañías telefónicas fueron las primeras en ofrecer el servicio de acceso a Internet a través de sus redes de cobre, pero con el paso del tiempo las compañías de cable las desplazaron, ya que podían ofrecer conexiones dedicadas y mucho más veloces a través de su red. La misma tendencia se dio en casi todo el mundo.

vertical y horizontalmente para llegar acaparar todo el mercado de telefonía en ese país en los años ochenta, hasta el punto de llegar a impedir que un tercero produjera teléfonos o aplicaciones para conectar a su red.[14]

Es este ejemplo de los teléfonos –conocido como el episodio *Hush-a-phone*– el que Wu usó en su texto de 2003 para agregar un elemento al riesgo de integración en las empresas de cable: la discriminación de contenidos también era un problema de innovación. «El principio básico detrás de un régimen antidiscriminación para una red es darles a los usuarios el derecho a usar aplicaciones y accesorios no perjudiciales, y a los innovadores, la libertad correspondiente para ofrecerlos».[15]

El tiempo le dio la razón a los más pesimistas. En 2003, el Noveno Circuito de la Corte de Apelaciones de Estados Unidos clasificó el servicio de Internet por cable como de telecomunicaciones, lo que implicaba que los proveedores no podían discriminar el contenido y debían interconectarse. Hasta ahí, todo bien: eran transportadores comunes (*common carriers*), como las compañías telefónicas. Pero, paralelamente, la Comisión Federal de Comunicaciones (CFC) declaró que el de Internet por cable era un servicio de información, lo cual sacaba a las compañías de cable de la categoría de telecomunicaciones y, por ende, las eximía del régimen de transporte común.[16]

La discusión la terminó zanjando la Corte Suprema de ese país. En una opinión de junio de 2005, argumentó que si bien las compañías de cable ofrecían acceso a Internet, lo hacían en conjunción con servicios de información –los canales de televisión– por lo cual no estaban sujetas a un régimen de transporte común. Así, la Corte le dio la razón a la CFC y dejó el servicio de banda ancha, en esencia, desregulado.[17]

El argumento sorprendió al juez conservador Antonin Scalia, que en su escrito disidente manifestó que si bien los servicios informativos y de telecomunicaciones estaban empaquetados, era perfectamente posible identificar el de acceso a Internet como uno independiente que debería estar sujeto a las

---

[14] Para un recuento detallado, ver Wu, *supra* nota 6.

[15] Wu, *supra* nota 7, ps. 142-143. Traducción informal.

[16] Cfr. Crawford, S., *Captive Audience,* Yale University Press, 2013.

[17] Cfr. Corte Suprema de Justicia de Estados Unidos, *Nat'l Cable & Telecommunications Ass'n v. Brand X Internet Services,* 27 de junio de 2005, disponible en: http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=US&navby=case&vol=000&invol=04-277#opinion1 (consultada el 15 de octubre de 2013).

provisiones generales de «llevar sin preguntar». Para Scalia, este caso no era comparable al de una pizzería, donde el servicio de entregas a domicilio está necesariamente atado al de la oferta de pizza.[18]

En ese mismo año, la CFC adoptó una Declaración de política pública sobre neutralidad de la red. Allí estableció que los usuarios de Internet tienen derecho a acceder a cualquier contenido legal de su elección; a ejecutar aplicaciones y usar servicios de su elección; a conectar los dispositivos legales de su elección que no dañen la red, y a gozar de la competencia entre los operadores de redes, de aplicaciones, de servicios y de contenidos. Sin embargo, sujetó estas prerrogativas a la potestad de los PSI de hacer una «gestión razonable de la red» y a las necesidades en materia de aplicación de la ley.[19]

Para Susan Crawford –que fue asesora del gobierno de Obama en temas de tecnología e innovación– la posición de la CFC, avalada por la Corte, creó el riesgo de que las empresas de cable discriminaran a favor de ciertos servicios en línea y en contra de otros.[20]

La prueba no tardó en llegar, en 2007 la Electronic Frontier Foundation documentó la manera como Comcast –el operador de cable que domina el mercado norteamericano– estaba afectando el uso de la red de pares BitTorrent. «La mayoría [de usuarios] culpaban a sus propios computadoras o al clima o a otra serie de elementos. Pocos adivinaban que su proveedor de acceso a Internet estaba bloqueando la habilidad para compartir archivos de video».[21]

La situación no ha cambiado mucho desde entonces. Con la llegada de Barack Obama al gobierno, la CFC trató tibiamente de encauzar a los operadores en el marco de neutralidad de la red, pero fue enfrentado con un *lobby* intensivo y una escalada judicial de parte de las compañías. En 2010, un extenso proceso de consulta terminó con un reporte de la CFC que mantuvo las excepciones amplias y subjetivas y, de paso, autorizó a los operadores móviles a discriminar aplicaciones de terceros en su plataforma (los

---

18 Cfr. Scalia, A., Escrito disidente, Nº 04-277 y 04-281, disponible en: http://www.law.cornell.edu/supct/html/04-277.ZD.html (consultada el 15 de octubre de 2013).

19 Cfr. Comisión Federal de Comunicaciones, Policy Statement, agosto 5 de 2005, FCC 05-151.

20 Cfr. Crawford, *supra* nota 16.

21 *Ibídem*, pos. 1076 (edición Kindle).

detalles de la regulación se mencionan más adelante).[22] En ese contexto, los operadores de banda ancha fija –cuyo servicio viene adoptando el 80 por ciento de los consumidores que se pasan a Internet de alta velocidad– pueden establecer «servicios gestionados» y cargos por consumo.

IV. El caso contra la neutralidad

Tal vez la posición más elaborada en contra de la neutralidad de la red proviene del académico Christopher Yoo, para quien la arquitectura original no resulta apta para el Internet de ahora y de mañana. Yoo basa su argumento en cuatro cambios fundamentales en los últimos años: i) el incremento en el número y diversidad de usuarios, ii) el incremento en la diversidad e intensidad de las aplicaciones, iii) el incremento en la variedad de tecnologías, y iv) el desarrollo de relaciones comerciales más complejas en el entorno digital.

«El dramático giro en el uso de Internet sugiere que los principios fundacionales de mediados de los noventa pueden no ser apropiados hoy», afirma Yoo, y propone una aproximación diferente a la de la neutralidad de la red: «En vez de ofrecerle a los usuarios finales un único producto uniforme, distintas porciones de la red pueden responder de diferentes maneras, ofreciéndoles a los usuarios una variedad de servicios para escoger –una práctica que yo he llamado “diversidad de la red”–».[23]

La idea de que el diseño original de Internet no se ajusta del todo a ciertos servicios y aplicaciones es cierta. Aunque la regla del «mejor esfuerzo» en el envío de paquetes –según la cual el éxito depende, entre otros, del tráfico de la red– es suficiente para servicios como el correo electrónico, no lo es para la telefonía en Internet o las transmisiones en vivo. En su versión original, la red no puede garantizar una calidad óptima del servicio (*quality of service, QoS*).[24]

---

[22] Cfr. Comisión Federal de Comunicaciones, *In the Matter of Preserving the Open Internet Broadband Industry Practices. Report and Order,* GN Docket Nº 09-191, WC Docket Nº 07-52, 23 de diciembre de 2010.

[23] Yoo, Christopher, *The Dynamic Internet: How Technology, Users, and Businesses are Transforming the Network,* AEI Press, 2012, pos. 192 y 231-237 (versión Kindle). Traducción informal.

[24] Lessig, L., *The Future of Ideas.The Fate of the Commons in a Connected World,* Vintage, Random House.

De la misma forma, como plantea Yoo, la red original no fue concebida para el número exponencial de usuarios y servicios de hoy en día. Gestionar el tráfico no solo es buena idea sino necesario –dicen los contradictores–, especialmente cuando algunos usuarios hacen un uso excesivo de la red. Es lo que se conoce como «la tragedia de los bienes comunes»: actuando racional e individualmente, cada actor agota el recurso en detrimento de los intereses comunes del grupo.[25] El ejemplo típico en Internet es el de un adolescente que usa su ancho de banda para descargar de manera permanente e ininterrumpida videos, juegos y canciones, lo cual afecta a las personas que comparten la última milla de esa conexión.

La neutralidad de la red también suele plantearse como un obstáculo para quienes consideran prioritario combatir la inseguridad en línea. Más allá de las soluciones propuestas, es una realidad que el software malicioso se campea en Internet, que las violaciones de datos personales ocurren con frecuencia y que los ataques a la infraestructura crítica son un riesgo constante.[26]

Todos estos aspectos están atravesados por un innegable interés comercial, que capitaliza varios de estos argumentos y a la vez los moldea. Algunos PSI en Estados Unidos han llegado a afirmar que obligarlos a ser neutrales en sus redes es una forma de expropiación.[27] Y, en general, todos consideran que como parte de su libertad económica es necesario ofrecer servicios segmentados para un mercado de consumidores que no está siendo atendido. No hacerlo les impedirá expandir las redes y –dicen– construir las del futuro. Con neutralidad de la red no habrá ni incentivos ni ingresos.[28]

Lo cierto es que por una u otra razón los PSI han desplegado tecnologías que desconocen la arquitectura original de la red y reconfiguran –sobre la marcha y sin mayor discusión– los principios que la orientan. Desde el punto de vista técnico, hay varias formas de hacerlo. Según Van Schewick,

---

[25] Cfr. Hardin, G., «The Tragedy of the Commons», *Science*, 162, 1968, ps. 1243-1248, disponible en: http://www.sciencemag.org/content/162/3859/1243.full (consultada el 16 de octubre de 2013).

[26] Cfr. Deibert, R., *Black Code: Inside the Battle for Cyberspace*, McClelland & Stewart, 2013.

[27] Cfr. Marsden, *supra* nota 5, p. 48.

[28] Sobre estos argumentos, ver Belli, L., «Network Neutrality and Human Rights», Background Paper, CERSA, Pres Sorbonne University, mayo de 2013. También, Crawford, *supra* nota 16, y Van Schewick, *supra* nota 2.

el principio de extremo a extremo, por ejemplo, se puede ignorar de dos maneras: al implementar en el núcleo de la red funcionalidades relativas a las aplicaciones, o al incrementar la capacidad de los administradores de la red para controlar las aplicaciones y contenidos que pasan por sus tubos.[29] Esto es, al volver centralizado un esquema descentralizado.

En otras palabras, los proveedores quieren asumir un rol central y tener ojos en la red. Al añadir protocolos relacionados con aplicaciones en el nivel más bajo, aumenta la capacidad de monitorear. Esto puede hacerse a través de dispositivos y tecnologías que hagan la red más consciente de lo que transporta para así tomar decisiones. La «inspección profunda de paquete» es la tecnología más empleada para este fin.[30]

En un estudio de 2012, el Cuerpo de Reguladores Europeos para Comunicaciones Electrónicas (BEREC, por sus siglas en inglés) documentó las prácticas de gestión de tráfico.[31] BEREC encontró varios casos en que los proveedores de acceso o tránsito del servicio de Internet sofocan o bloquean el flujo de cierto tipo de tráfico. Mientras el bloqueo implica que el usuario no puede acceder al contenido o servicio deseado, el sofocamiento o *throttling* no conlleva la interrupción total de la conexión, sino una reducción en la velocidad de ésta o la pérdida de una solicitud al servidor –recuérdese el principio del «mejor esfuerzo»–. Esto último lo evidencia el usuario porque, por ejemplo, la página a la que intenta acceder no carga o el archivo que está descargando se estanca o se vuelve más lento.

Los casos más frecuentes de *throttling* y bloqueo se hacen en redes de pares (*peer-to-peer* o P2P) y en servicios de voz sobre IP. Las redes de pares –como BitTorrent o Ares– conectan directamente a un usuario con otro, y sirven para intercambiar archivos sin necesidad de pasar por un servidor (donde deben subirse y descargarse). La voz sobre IP, por su parte, permite que a través de Internet se transmitan servicios de comunicaciones –voz, texto, mensa-

---

29 Cfr. Van Schewick, *supra* nota 2, pos. 3587.

30 Para una explicación detallada sobre el *deep packet inspection,* ver op. cit. Cortés Castillo.

31 Cfr. Cuerpo de Reguladores Europeos para Comunicaciones Electrónicas, «A view of traffic management and other practices resulting in restrictions to the open Internet in Europe», *BoR* (12)30, mayo 29 de 2012, disponible en: http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf (consultada el 16 de octubre de 2013).

jes–, los cuales compiten directamente con los que se ofrecen a través de la telefonía básica conmutada o la red celular.

Además de estas dos categorías, el informe de BEREC reporta situaciones de priorización de tráfico, degradación de otro, bloqueo de puertos y manejo de congestión de la red. Esto último se hace tanto a través de aplicaciones que no discriminan según el tipo de tráfico como de aquellas que sí lo hacen –en cuyo caso se trata de medidas estrechamente relacionadas con el sofocamiento–.

El propósito de este documento no es resolver el debate entre promotores y opositores de la neutralidad de la red (está claro, por demás, que acá se asume una posición favorable a ésta). Sin embargo, vale la pena cerrar este capítulo señalando algunos contra-argumentos a lo que hemos expuesto hasta aquí.

El informe de BEREC se basa en un temor fundado al que ya hemos hecho referencia: más allá de la legislación de cada país, «hay creciente preocupación de que los operadores de telecomunicaciones y prestadores del servicio de Internet (PSI) están explotando las técnicas de gestión de redes para favorecer a sus aliados comerciales o los servicios y aplicaciones con los que están integrados verticalmente».[32]

Para Lawrence Lessig, el verdadero peligro de alejarse de la neutralidad de la red está en las consecuencias imprevistas. Permitir la discriminación del tráfico en Internet supone entregarle al administrador de la red el poder de favorecer cierto tipo de contenido y, lo que es peor, el de restringir otro. En esa medida, Lessig propone una presunción a favor de la arquitectura original, que es la que ha permitido una extraordinaria interconexión, participación e innovación.[33]

Que Internet deje de ser una «red tonta con extremos inteligentes» no implica que no vaya a haber nuevas aplicaciones y desarrollos inesperados, pero sí será más costoso y menos democrático hacerlo. En la medida en que los dueños de la red establezcan reglas distintas para aplicaciones y servicios, serán ellos el primer cuello de botella para los entrantes. Y no hay interés más vital para el incumbente que protegerse de las amenazas de los entrantes.[34]

---

32 Belli, *supra* nota 28, p. 5. Traducción informal.

33 Cfr. Lessig y Lemley, en Marsden, *supra* nota 5, p. 53.

34 Cfr. Wu, *supra* nota 7, y Crawford, *supra* nota 16.

Esa centralización conllevará el estrechamiento del entorno digital y la restricción de derechos fundamentales, como la libertad de expresión y la privacidad.[35] De alguna forma este proceso ya está en marcha. El monitoreo de contenidos y usuarios no es una simple estrategia comercial en los términos expuestos por Yoo y otros autores, sino que hace parte de las denominadas arquitecturas de control, configuraciones granulares que buscan implementar protocolos de identificación y autenticación –tanto de individuos como de aplicaciones– a lo largo de toda la red.[36] Un propósito que, sin duda, riñe con el espíritu de la neutralidad.

V. Un vistazo a la regulación

Según Luca Belli, la base de una política pública sobre neutralidad de la red comprende dos dimensiones. La primera se centra en la necesidad de regular el manejo del tráfico de Internet y de limitar la habilidad de los operadores de la red de priorizar distintos flujos de datos. La segunda dimensión se enfoca en el propósito de que los recursos conectados a Internet sean universales y recíprocamente accesibles para todos.[37]

La obligación de no discriminación la proponen varios autores –entre ellos Dawn Carla Nunziato y Tim Wu–. Esta está estrechamente relacionada con la obligación de transporte común o *common carriers,*[38] y está presente en la mayoría de legislaciones o proyectos de ley en la materia. «En el corazón del transporte común está la idea de que ciertos negocios están ya sea íntimamente conectados, incluso son esenciales, al bien común, o son tan inherentemente poderosos –imagine el servicio de agua o electricidad– que deben estar obligados a conducir sus asuntos de manera no discriminatoria».[39]

---

[35] Cfr. Belli, *supra* nota 28.

[36] Cfr. Cohen, Julie E., *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, Yale University Press, 2012.

[37] Cfr. Belli, *supra* nota 28.

[38] Cfr. Nunziato, C., «Preservar la libertad en Internet en las Américas», en Bertoni, Eduardo (comp.), *Hacia una Internet libre de censura. Propuestas para América Latina*, Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Facultad de Derecho, Universidad de Palermo, 2012, ps. 11-45.

[39] Op. cit. Wu, *supra* nota 7, p. 58.

V.A. Estados Unidos

En 2010, la Comisión Federal de Comunicaciones de Estados Unidos incluyó este elemento en los cuatro principios para preservar el Internet abierto. No obstante, no prohibió escuetamente la discriminación, sino únicamente aquella que sea «no razonable». La CFC también incluyó los principios de transparencia, no bloqueo y gestión razonable de la red. Es ese adjetivo –«razonable»– lo que autores como Crawford consideran una carta blanca para que los prestadores incurran en todo tipo de actividades discriminatorias (sumado a que, como se explicó, las empresas de cable que ofrecen el servicio de banda ancha no son consideradas como transportadores comunes en ese país).[40]

Estos principios son todavía más débiles en el ámbito de Internet móvil. Para la CFC, la banda ancha móvil presenta características diferentes a la fija, ya que los operadores móviles tienen «limitaciones operativas» y, generalmente, ofrecen velocidades y capacidades más bajas. Bajo este supuesto, la comisión limitó los principios al deber de transparencia y no bloqueo, que de cualquier forma no obsta para que los operadores móviles hagan una gestión razonable de la red. La CFC se cuidó de establecer prohibiciones o deberes absolutos en Internet móvil. Por ejemplo, el deber de no bloquear no aplica cuando el proveedor excluya de su tienda de aplicaciones o equivalente aquellos servicios que puedan competir con el suyo.[41]

V.B. Europa

En Europa, el Cuerpo de Reguladores Europeos para Comunicaciones Electrónicas (BEREC) tomó la posición contraria, y en respuesta a una consulta de la Comisión Europea, manifestó: «Los principios que gobiernan la gestión de tráfico deben ser los mismos para redes móviles y fijas. Tanto los operadores móviles como los fijos enfrentan los mismos problemas técnicos en la administración de su red, y usan la misma tecnología basada en IP».[42]

BEREC reconoce que un operador móvil puede estar obligado a tomar medidas para mantener la capacidad de las celdas, en cuyo caso podrá estable-

[40] Cfr. Comisión Federal de Comunicaciones, *supra* nota 22.

[41] Cfr. *ibídem*.

[42] Cuerpo de Reguladores Europeos para Comunicaciones Electrónicas, «BEREC Response to the European Commission's consultation on the open Internet and net neutrality in Europe», *BoR* (10)42, 30 de septiembre de 2010.

cer topes de consumo en momentos dados. Esto, sin embargo, no debe desembocar en un tratamiento selectivo de contenidos.

En relación con la neutralidad en general, el Comité de Ministros del Consejo Europeo adoptó en 2010 una declaración según la cual los usuarios deben tener el mayor acceso posible al contenido en línea y a las aplicaciones y servicios de su elección, sin importar si son pagos o gratuitos. Esta potestad –agrega la declaración– incluye la elección del cualquier dispositivo compatible, y debe aplicar sin importar la infraestructura o la red a través de la cual el usuario accede a Internet.[43]

No son muchos los Estados europeos que han avanzado a partir de estas orientaciones. Entre otros, en el Reino Unido el regulador (OFCOM) ha tratado de llegar a un acuerdo con los prestadores para alcanzar una solución por la vía de la autorregulación, y en Francia, la autoridad competente (ARCEP) expidió una serie de recomendaciones al parlamento de ese país, entre las que se destaca la necesidad de adoptar reglas más allá de la transparencia y la competencia.[44]

Hasta el momento solamente Eslovenia y Holanda cuentan con leyes de neutralidad de la red. Holanda fue el primer país europeo en regular, en diciembre de 2012, a través de la Ley de Telecomunicaciones. Esta dispone que los proveedores de Internet no pueden establecer cobros de conexión a partir de los servicios que se ofrezcan en la red. Esta prohibición se complementa con varias restricciones en materia de gestión de tráfico.[45]

V.C. América Latina

Colombia, Chile y Perú tienen leyes que regulan la neutralidad de la red, pero solo Chile tiene una norma exclusiva sobre el tema. Comencemos por

---

[43] Cfr. Committe of Ministers, «Declaration of the Committee of Ministers on network neutrality», adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies, disponible en: http://archive1.diplomacy.edu/poolbin.asp?IDPool=1204 (consultada el 13 de octubre de 2013).

[44] Cfr. Marsden, C., *Net Neutrality Law: Past Policy, Present Proposals, Future Regulation? Proceedings of the United Nations Internet Governance Forum: Dynamic Coalition on Network Neutrality,* Nusa Dua Bali, Indonesia, 2013, disponible en: http://ssrn.com/abstract=2335359 (consultada el 16 de octubre de 2013).

[45] Cfr. Ley de Telecomunicaciones de Holanda, artículo 7.4a y ss., disponible en: http://www.government.nl/files/documents-and-publications/notes/2012/06/07/dutch-telecommunications-act/tel-com-act-en-versie-nieuw.pdf (consultada el 16 de octubre de 2013).

Colombia, el Plan Nacional de Desarrollo de 2011 incluye una protección que parece completa. No obstante, a la manera de la regulación norteamericana, incluye una excepción a la discriminación:

> «[Los PSI] no podrán bloquear, interferir, discriminar, ni restringir el derecho de cualquier usuario de Internet, para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio lícito a través de Internet. En este sentido, deberán ofrecer a cada usuario un servicio de acceso a Internet o de conectividad, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de estos. *Los prestadores del servicio de Internet podrán hacer ofertas según las necesidades de los segmentos de mercado o de sus usuarios de acuerdo con sus perfiles de uso y consumo, lo cual no se entenderá como discriminación*» (énfasis agregado).[46]

Esta norma también incluye la libertad de conectar dispositivos –«siempre que sean legales y que los mismos no dañen o perjudiquen la red o la calidad del servicio»– y la obligación de transparencia e información.[47]

Un paréntesis relevante: la obligación de transparencia mereció especial atención en la declaración conjunta de los relatores de libertad de expresión acerca de Internet. Además de hablar del deber de no discriminación en el punto de neutralidad de la red, los relatores –entre los cuales está la Relatora Especial de la Comisión Interamericana de Derechos Humanos– manifestaron que «se debe exigir a los intermediarios de Internet que sean transparentes respecto de las prácticas que emplean para la gestión del tráfico o la información, y cualquier información relevante sobre tales prácticas debe ser puesta a disposición del público en un formato que resulte accesible para todos los interesados».[48]

Volviendo al panorama legislativo, la ley 20.453 de Chile establece la misma garantía de no discriminación (la ley colombiana parece haber copia-

---

[46] Plan Nacional de Desarrollo de Colombia, ley 1450 de 2011.

[47] De acuerdo con el numeral 4 del artículo 56 de la ley 1450, los PSI «publicarán en un sitio web toda la información relativa a las características del acceso a Internet ofrecido, su velocidad, calidad del servicio, diferenciando entre las conexiones nacionales e internacionales, así como la naturaleza y garantías del servicio».

[48] «Relatorías de Libertad de expresión emiten declaración conjunta acerca de Internet», Comunicado de Prensa R50/11, Relatoría Especial para la Libertad de Expresión, disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=848&lID=2 (consultada el 18 de octubre de 2013).

do la chilena), pero su excepción parece más estrecha que las demás mencionadas: «los concesionarios de servicio público de telecomunicaciones y los proveedores de acceso a Internet podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red, en el exclusivo ámbito de la actividad que les ha sido autorizada, siempre que ello no tenga por objeto realizar acciones que afecten o puedan afectar la libre competencia».[49]

En contraste con la mayoría de normas revisadas, la peruana incluye expresamente el término «neutralidad de la red» y no establece ninguna excepción a la prohibición de discriminación. Según el artículo 6 de la Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica, «los proveedores de acceso a Internet respetarán la neutralidad de red por la cual no pueden de manera arbitraria bloquear, interferir, discriminar ni restringir el derecho de cualquier usuario a utilizar una aplicación o protocolo, independientemente de su origen, destino, naturaleza o propiedad».[50]

En el resto de la región hay proyectos de ley en curso o regulaciones de menor entidad –decretos y resoluciones–. Entre otros, el proyecto Marco Civil en Brasil incluye un artículo sobre la neutralidad de la red;[51] en Argentina, la Secretaría de Comunicaciones abordó el tema en una resolución,[52] y en Ecuador hizo lo propio el Consejo Nacional de Telecomunicaciones.[53]

VI. Conclusión

En los últimos años, la neutralidad de la red ha pasado de ser un concepto difuso y general a uno con contenido y sustento legal. Aunque no existe una

---

49 Ley 20.453 de 201 de Chile, artículo 24.H.a, parágrafo segundo.

50 Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica de Perú, disponible en: https://dl.dropboxusercontent.com/u/199729/Ley_Banda_Ancha_TS.pdf (consultada el 16 de octubre de 2013).

51 Cfr. Proyecto de Marco Civil de Internet de Brasil, disponible en: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=912989&filename=PL+2126/2011 (consultada el 16 de octubre de 2013).

52 Cfr. Secretaría de Comunicaciones de Argentina, Resolución Nº 5 de 2013, disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/215000-219999/216915/norma.htm (consultada el 16 de octubre de 2013).

53 Cfr. Consejo Nacional de Telecomunicaciones de Ecuador, Resolución Tel-477-16-CONATEL-12, disponible en: http://www.telconet.net/archivos/Reglamento_Abonados.pdf (consultada el 16 de octubre de 2013).

definición unívoca en las leyes alrededor del mundo, parece haber un piso común: la neutralidad incluye la no discriminación de contenidos, la garantía de no bloqueo y la libertad de uso de dispositivos.

El punto más complicado parece estar en la excepción del derecho de los PSI a gestionar su red. Esta excepción parecería quedar clara en conjunción con la obligación de no discriminación. Es decir, puede gestionarse el tráfico de la red siempre y cuando no implique la discriminación de un tipo de paquetes en particular. Pero el asunto no queda resuelto ahí: antecedentes como el de Estados Unidos indican que bajo la sombrilla de la «gestión razonable» caben todo tipo de prácticas discriminatorias.

En muchos casos, estas prácticas no son realmente excepciones, sino un servicio distinto (especialmente en el Internet móvil). Y aunque allí parece abrirse una grieta en la idea de neutralidad, puede ser a la postre una oportunidad. Según Marsden, cada vez más los prestadores del servicio de Internet están creando servicios gestionados en carriles paralelos al Internet público –donde ofrecen calidad del servicio (QoS), en contraposición al «mejor esfuerzo»–.[54]

Ante una realidad comercial como esa, tal vez sea importante reconocer esa práctica como algo externo a la neutralidad. Hacerlo no está exento de riesgos, pero puede servir para avanzar. Sobre el particular, la Coalición Dinámica para la Neutralidad de la Red publicó un modelo regulatorio que contempla ese punto en los siguientes términos:

> «El principio de neutralidad de la red no necesita ser aplicado hacia servicios especializados. Se debe permitir que proveedores de servicio de Internet ofrezcan servicios especiales además de acceso a servicio de Internet, a condición de que estas ofertas no afecten negativamente el acceso a Internet, su rendimiento, accesibilidad o calidad. Ofertas para brindar servicios especializados deben ser proporcionadas sin discriminación y su adopción por parte de los usuarios de Internet debe ser voluntaria».[55]

Excluir los servicios especializados de las excepciones a la neutralidad de la red fortalece la definición de ésta y facilita su implementación como polí-

---

[54] Cfr. Marsden, *supra* nota 44.

[55] Dynamic Coalition on Network Neutrality, «Model Framework on Network Neutrality», disponible en inglés en: http://networkneutrality.info/sources.html, y en español en: http://www.palermo.edu/cele/noticias/cele-neutralidad-red.html (consultada el 18 de octubre de 2013).

tica pública. Adicionalmente, conciliaría algunas de las visiones críticas sobre neutralidad como sinónimo de bloque a la innovación y el desarrollo de la red.

Esta propuesta, decimos, no está exenta de riesgos. El hecho de que el acceso a Internet se ofrezca paralelamente con una red de servicios especializados, podría en últimas afectar Internet. Los prestadores podrían terminar degradando el servicio hasta establecer redes de primera y segunda categoría. No obstante, la incorporación masiva y democrática del Internet que conocemos, con el apoyo gubernamental, ayudaría a mantener el entorno digital en un estado adecuado para el intercambio democrático de información, el debate público y la innovación descentralizada.

Ese rol oficial se concreta de muchas maneras, y aunque no es el propósito de este documento hablar de la implementación de las leyes sobre neutralidad de la red, es importante hablar de la vigilancia y el control. Aun en los países con regulación en la materia, las prácticas de los proveedores indican que es poco o nada lo que el Estado hace para evitar que se viole la neutralidad de la red. Esto puede deberse a muchas causas: el regulador no tiene fortaleza para intervenir o no cuenta con la capacidad para documentar las irregularidades; el proveedor del servicio no tiene incentivos suficientes para cumplir, o el usuario en general no exige un servicio en términos acordes con la neutralidad.

De una u otra forma, la puesta en práctica de la neutralidad de la red merece más atención, y así como la sociedad civil viene trabajando en los marcos regulatorios es preciso que examine en mayor detalle la mejor manera de llevarlos a la práctica.

VII. Recomendaciones

• La regulación sobre neutralidad de la red debe estar contenida en una ley expedida por los congresos de los Estados. Solo así se garantiza un debate adecuado y amplio sobre las características y el alcance de una ley en la materia.

• Las excepciones a la neutralidad de la red deben establecerse en conjunción con la obligación de no discriminación. De lo contrario, bajo categorías como la «gestión razonable» se termina desvirtuando la garantía de neutralidad.

• La idea de reconocer los servicios especializados ofrecidos por los prestadores del servicio de Internet como algo distinto al Internet abierto, puede a la postre fortalecer el concepto de neutralidad de la red. Propuestas como la de la Coalición Dinámica por la Neutralidad de la Red deben ser parte de las discusiones en materia de política pública.

• Relacionado con lo anterior, la posibilidad de que existan paralelamente servicios preferenciales y el Internet abierto no puede, de ninguna manera, desembocar en la degradación de esta última.

• La implementación de las normas sobre neutralidad de la red merecen tanta atención como su diseño. Debe trabajarse en la documentación de casos y en la labor de monitoreo del gobierno.

• Los principios sobre neutralidad de la red parecen perder vigencia en el ámbito de los servicios móviles. Teniendo en cuenta que el acceso a Internet va moviéndose paulatinamente a las plataformas móviles, es importante que el trabajo de la sociedad civil y de los reguladores se centre también en este aspecto.

Vigilancia de la red: ¿qué significa monitorear y detectar contenidos en Internet?[1]

Resumen

Este documento analiza el creciente interés de los gobiernos en monitorear la red.[2] En primer lugar, ofrece un marco conceptual general sobre la arquitectura de Internet. Posteriormente, analiza el concepto de control en Internet, haciendo énfasis en los intermediarios y en el uso de tecnologías como la Inspección Profunda de Paquete. Por último, plantea la tensión entre la seguridad nacional y la prevención de la violencia, y derechos como la libertad de expresión y la privacidad.

La conclusión de este documento es que el monitoreo de los contenidos en línea pone en riesgo las garantías fundamentales de los ciudadanos y amenaza con desmontar el entorno digital abierto y pluralista que conocemos. Y se hacen, entre otras, las siguientes recomendaciones:

- Necesidad de amplia participación y consulta: las discusiones de proyectos de ley sobre monitoreo de contenidos en Internet que se lleven a cabo deben

---

[1] Este documento fue elaborado por Carlos Cortés Castillo, investigador de la Iniciativa por la Libertad de Expresión en Internet (iLEI), del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo. La investigación y elaboración del documento fue dirigida y contó con los comentarios de Eduardo Bertoni, director del CELE.

[2] En buena medida, decidimos estudiar este tema luego de conocer la existencia de algunos proyecto de ley argentinos que buscan establecer mecanismos de detección o monitoreo de contenidos en Internet. Se trata de los proyecto de ley 728 y 1892, ambos de 2012. No obstante, la relevancia del tema –y, por ende, del documento– tiene un indudable alcance regional.

contar con una participación amplia, que garantice la inclusión de todos los puntos de vista y un adecuado nivel de conocimiento sobre los temas técnicos.

- Necesidad de estudios de impacto a derechos humanos: en relación con la recomendación anterior, sugerimos que los proyectos de ley que buscan establecer mecanismos de monitoreo de contenidos en Internet cuenten con un estudio técnico previo sobre el impacto que tendrían en materia de derechos humanos y en la arquitectura de la red. Los resultados de éste deben explicitarse en la exposición de motivos de la iniciativa.
- Necesidad de transparencia e información de los PSI y OSL: los Proveedores de Servicios de Internet y los Operadores de Servicios en Línea deben informarles a sus usuarios cómo y en qué condiciones monitorean sus contenidos. Esta obligación incluye el uso de tecnologías como la Inspección Profunda de Paquete.
- Transparencia e información de los gobiernos: los gobiernos deben hacer explícitas las políticas de vigilancia y monitoreo de Internet, bien sea en desarrollo de leyes existentes o de decisiones administrativas. Específicamente, deben ser transparentes con las obligaciones que imponen a los intermediarios.
- Necesidad de delimitar el uso de herramientas de monitoreo**:** las autoridades judiciales y de inteligencia pueden contar con herramientas legales para monitorear la actividad en línea de los ciudadanos. Sin embargo, éstas deben estar sujetas a las mismas restricciones que se aplican en otros temas, como la protección de datos y la interceptación de comunicaciones.
- Necesidad de ampliar el debate con los usuarios: las organizaciones de la sociedad civil que trabajan en estos temas deben hacer un esfuerzos por acercar a los usuarios a este debate. Esto incluye la formación en herramientas legales y derechos humanos aplicadas a Internet.

I. Introducción

La primera persona en usar el término «ciberespacio» para referirse a Internet fue John Perry Barlow, en 1996: «Gobiernos del Mundo Industrial, ustedes, gigantes cansados de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, les pido a ustedes, del pasado, que nos dejen en paz. No son bienvenidos entre nosotros. No tienen soberanía donde nos reunimos».[3] Su declaración era un rechazo a la intromisión de los Estados en la

[3] Barlow, J. P., «A Declaration of Independence of Cyberspace», disponible en: https://projects.eff.org/~barlow/DeclarationFinal.html (consultada el 19 de junio de 2012). Traducción informal.

naciente red, y se convertiría en el manifiesto libertario de los años siguientes. Los «ciberlibertarios» –como eran conocidos– exigían un Internet autónomo, alejado de las instituciones políticas y legales del mundo real.[4]

Vistas en retrospectiva, las palabras de Barlow fueron proféticas, tanto por la visión que tenía de un entorno digital revolucionario –un auténtico ciberespacio–, como por el temor que albergaba de una intervención estatal. Y es este último punto el que convirtió su manifiesto en una utopía: hoy en día, y de manera creciente, todo tipo de normas regulan actividades en Internet, desde las transacciones comerciales hasta el acceso a material pornográfico. Esto sin mencionar el pulso por la regulación de la infraestructura de la red, o los debates sobre las instituciones internacional que deben hacerse cargo de su gobernanza.

Aunque Internet es un territorio en disputa, los Estados reivindican su soberanía sobre la fracción de cables, tubos y señales que pasa por sus fronteras. Y en ese propósito, una de las obsesiones de los Estados es controlar los contenidos a los que acceden sus ciudadanos. El ejemplo más célebre es el de China, que cuenta con un cortafuegos (o *firewall)* tan impresionante como su legendaria muralla. Entre el Internet que conocemos en Occidente y al que acceden en China se interpone un sofisticado sistema de filtros y bloqueo de contenidos. Algo similar sucede en Irán, donde varios servidores intermediarios (o *proxys*) monitorean los datos que transmiten los usuarios.[5]

La explicación usual que oímos frente a estas iniciativas es que se trata de una estrategia de censura oficial: esos gobiernos ocultan información que, de conocerse, minaría las bases de su propia legitimidad y autoridad. En esencia, es un atentado contra la democracia. No obstante, el caso de estos países no sirve para explicar todas las intervenciones de los gobiernos en Internet. En muchos otros escenarios, los Estados defienden principios que las constituciones consagran y los ciudadanos exigen.

El ejemplo más reciente lo tenemos en Argentina. Un proyecto de ley presentado en el Congreso[6] propone la creación del Observatorio de Redes

---

[4] Cfr. Murray, A., «Nodes and Gravity in Virtual Space», *Legisprudence*, 5 (2), 2011, ps. 195221.

[5] Freedom House, *Freedom on the Net 2011,* Washington, 2011.

[6] Proyecto de ley 1892 de 2012. Tiene origen en la Cámara de Diputados. Fue publicado en el Trámite Parlamentario Nº 22 el 3 de abril de 2012. Se giró a tres comisiones: a) Derechos humanos y garantías, b) Comunicaciones e informática, y c) Presupuesto y Hacienda.

Sociales, de Correos Electrónicos y Mensajes de Texto, que busca «detectar, combatir y denunciar» expresiones de acoso, discriminación y violencia en Internet. En el mismo sentido de este proyecto, pero un paso más adelante, países como Alemania, Francia o Brasil han aplicado normas genéricas o específicas para prevenir la difusión en Internet de contenidos ofensivos o políticamente sensibles.

A primera vista, el verbo «detectar» que contiene el proyecto argentino parece referirse a un proceso de menor importancia. Tal vez se refiera a monitorear los contenidos que ya son públicos en la red, como foros de lectores en medios de comunicación o actualizaciones de estado en redes sociales. Tal vez sería más grave si se hablara de «bloquear» o «remover». Sin embargo, ¿qué implica detectar o monitorear contenidos en Internet?, ¿cuáles son las consecuencias para los ciudadanos?

Este proyecto argentino no contempla ningún mecanismo; se limita a exigir que los prestadores de servicios de Internet y de redes sociales ubiquen en un lugar visible los datos de contacto del Observatorio. No obstante, otro proyecto de ley que conoció el CELE[7] busca obligar a los establecimientos de comercio que ofrezcan conexión a Internet a que instalen obligatoriamente programas de detección y filtrado de contenidos no aptos para menores de edad.

Más allá de cado caso en particular, estas iniciativas dejan entrever un posible desconocimiento de parte de los legisladores de la manera como funciona Internet y del impacto que puede tener una norma, más allá de su intención, en los derechos fundamentales de las personas.

El propósito de este documento es, entonces, analizar ese deseo ascendente de los gobiernos de observar la red, y explorar la tensión entre estas iniciativas y derechos como la libertad de expresión y la privacidad. Igualmente, el propósito es delinear las implicancias de este objetivo en el ambiente digital.

Es necesario hacer varias precisiones sobre el alcance de este documento. En primer lugar, nos centraremos en el gobierno como actor principal. Muchos actores privados tienen intereses propios en que se monitoree cierto

---

[7] Se trata del proyecto de ley 728 de 2012, de Protección y Promoción de los Derechos de las Niñas, Niños y Adolescentes en Internet. Ingresó a la Dirección de Comisiones el 13 de abril de 2012 y fue enviado a tres comisiones el 16 de abril de 2012: a) De sistemas, medios de comunicación y libertad de expresión, b) De población y desarrollo humano, y c) De justicia y asuntos penales. Al 10 de julio de 2012, no tiene fecha de egreso de ninguna de las tres.

tipo de contenidos en Internet. Por ejemplo, la industria del entretenimiento viene haciendo cabildeo político y legal para que los intermediarios inspeccionen y retiren contenidos que supuestamente violan los derechos de autor. No obstante, ese enfoque no se abordará acá, ya que desbordaría el objetivo que nos proponemos. Lo anterior no implica que omitamos el papel de los proveedores de servicios de Internet, ya que son estos los que, por su ubicación estratégica, hacen parte de la estrategia oficial de monitorear la red.

En segundo lugar, nos enfocaremos en el problema del monitoreo en Internet. La filtración y el bloqueo de contenidos están estrechamente relacionados con este tema. Sin embargo, la idea de observar la red y detectar contenidos –en los términos que sugiere el proyecto argentino mencionado– sigue la línea de una tendencia que ya se ha visto en otros países. En términos técnicos, el monitoreo o detección se lleva a cabo mediante la Inspección Profunda de Paquete o *Deep Packet Inspection*, una tecnología que permite observar (muchas veces sin que el usuario sepa) todos los contenidos que pasan por la red.

En tercer lugar, este documento hace un uso extenso de analogías para explicar varios aspectos relacionados con Internet. Esta figura debe interpretarse de manera cuidadosa y, en particular en este documento, únicamente como un recurso pedagógico. Es usual que, en documentos y debates públicos, Internet se asimile en algunos aspectos al teléfono o a la televisión. Igualmente, se toman prestados elementos de dispositivos como el DVD o el VHS, o se asemeja el funcionamiento de la red a un correo postal o a una autopista. El problema consiste en que muchas veces estas analogías apuntan a negar regulaciones específicas para Internet dado que, justamente al acudir a ellas, ya existen normas aplicables. Y aunque Internet comparte semejanzas con cada uno de los ejemplos citados, ninguno lo explica completamente ni sirve como modelo para su regulación.

Por último, una advertencia que debe tenerse en cuenta durante todo el texto: para analizar cualquier tipo de política pública relacionada con Internet resulta indispensable entender antes cómo funciona. La premisa parece obvia, pero se desconoce constantemente en los debates sobre este tema. Tal omisión es justificable, al menos en parte, debido al alto nivel de sofisticación y tecnicismo que rodea Internet. Construir puentes entre las ciencias sociales (el Derecho y la Ciencia Política, entre otros) y la tecnología (la Ingeniería, los Sistemas) es un objetivo vital en el fortalecimiento de esta discusión.

Para lograr ese propósito fue necesario simplificar algunas explicaciones técnicas y omitir algunos conceptos. De otra manera, este documento no sería entendible para la mayoría del público para el cual está pensado. Un experto

podrá encontrar este enfoque falto de rigor, pero lo hemos hecho de manera cuidadosa, tratando de «traducir» el debate sin omitir sus elementos clave.

II. La arquitectura de la red

La característica más importante de Internet es que es una red descentralizada. En términos generales, no existen puntos de control por donde pasen todos los datos ni requisitos previos para que una persona envíe o reciba información –más allá de tener una computadora conectada a la red–. A esto se suma el manejo homogéneo de todos los datos que se transmiten y la posibilidad de hacer varios intercambios a través de una misma conexión.[8] Existen tres términos técnicos que explican esta arquitectura de Internet y que la diferencian de otros medios o sistemas de comunicación: i) el Principio de extremo a extremo o *Endtoend Principle*, ii) la conmutación de paquetes de datos o *packet switching*, y iii) el Modelo de Interconexión de Sistemas Abiertos u *Open System Interconnection*. A continuación ofrecemos una explicación breve de cada uno.

II.A. El Principio de extremo a extremo (PEE)

El PEE es un principio de diseño de redes según el cual las funciones o servicios de la red deben implementarse en los extremos de ésta. En el caso de Internet, hablamos de una «red tonta» (*dumb network*) con «inteligencia» en los extremos. Es decir, una red que se limita a transportar los datos hacia su destino, donde se encuentran las aplicaciones y dispositivos que los interpretan.[9] Esto permite que en la red «convivan» aplicaciones con funciones distintas de texto, voz, video o datos.

Puesto en práctica, el PEE se asemeja al funcionamiento de una autopista, con sus carreteras y caminos anexos. La autopista permite el tránsito de cualquier vehículo: no establece restricción al servicio que presta –transporte público o privado–, y es en su destino donde se diferencia –dejar a un pasajero, entregar una encomienda, etcétera–.

---

[8] Hablamos de un manejo homogéneo en términos generales. No obstante, los proveedores de servicios suelen aplicar políticas de manejo de tráfico o *traffic management* en su redes. Este punto será abordado más adelante.

[9] Cfr. Van Schewick, *Internet Architecture and Innovation*, The MIT Press, pos. 1098 y ss. (versión Kindle).

En los primeros años de Internet, la utilidad del PEE era menos perceptible, ya que todos las computadoras que usaban la red eran similares y, en general, cumplían las mismas funciones. Hoy en día la relevancia es clara: a Internet no se conectan solo las computadoras de escritorio, sino también portátiles, impresoras, dispositivos móviles (tabletas, teléfonos), radios y consolas de juego, entre otros. Igualmente, el menú de aplicaciones y usos crece exponencialmente cada minuto. Cada unos de estos aparatos y aplicaciones usa la conexión de manera diferente, lo cual es posible gracias a este principio.

II.B. La conmutación de paquetes de datos (*packet switching*)

Este método de comunicación –que complementa el PEE– divide y agrupa los datos que se transmiten a través de la red sin importar sus características. En otras palabras, para la red es tan «importante» el texto de un blog como una transacción financiera. Así, en el punto de origen de la transmisión los datos se parcelan en varios paquetes y viajan por la red en cualquier orden, dependiendo de factores como el tamaño (no es lo mismo ver un video en YouTube que enviar un correo electrónico), la velocidad de la conexión y la ruta entre emisario y destinatario. En el destino final, los paquetes se rearman en su estado original (para que una voz en Skype se entienda, por ejemplo) o de la manera adecuada para que sean accesibles (que un texto sea legible).

Para armar ese rompecabezas, cada paquete contiene dos tipos de información: una parte, conocida como el «encabezado», que permite determinar la ruta del paquete y, dependiendo del tipo, también la manera como se relaciona con los demás paquetes y las aplicaciones o programas que están involucrados (Outlook o Safari, por ejemplo). Y otra, conocida como la «carga útil», que contiene una porción de los datos objeto de la transmisión (una fracción del texto o el video como tal).[10] Usualmente los textos técnicos hablan de la pareja de protocolos TCP/IP, que constituyen la base de esta operación de conexión y transporte.[11]

[10] Cfr. Parsons, C., «Deep Packet Inspection in Perspective: Tracing its Lineage and Surveillance Potentials», *The New Transparency Project,* Working Paper 1, The Surveillance Project, disponible en http://qspace.library.queensu.ca/handle/1974/1939 (consultada el 19 de junio de 2012).

[11] Sin embargo, no son los únicos protocolos.

Además de los cables, los tubos y los computadores de los usuarios, este intercambio de información se logra mediante el uso de enrutadores o *routers*. El enrutador es un equipo que interpreta datos (como el que tenemos en nuestra casa, usualmente debajo del escritorio) conectado a dos o más líneas de la red cuya función es recibir paquetes de datos y enviarlos a otro enrutador, que repite la función hasta que los datos llegan a su destino. Los enrutadores están en todos los puntos de la red: en los simples, como la casa o la oficina, o en sitios críticos, como las instalaciones de los Prestadores de Servicios de Internet (PSI), agencias de gobierno o núcleos de conexión que constituyen la espina dorsal de la red. Básicamente, entre un cable y otro siempre hay un enrutador.

Siguiendo con la analogía anterior, la autopista –como la conmutación de paquetes en la red– alberga por igual buses, carros o camionetas. Dependiendo del peso y el tráfico, los autos toman una u otra ruta, y llegan a su destino gracias a la información que proporcionan las señales de tránsito a lo largo del camino –los enrutadores–.[12]

La conmutación de paquetes de datos permite que una red sea más eficiente y se utilice simultáneamente para transmitir todo tipo de información. Este método se diferencia de la conmutación de circuitos, donde la red establece un canal exclusivo entre dos extremos para que intercambien datos.

El ejemplo clásico de este último es la telefonía análoga que tuvimos hasta hace poco: cuando dos personas hablaban por teléfono se establecía un canal de comunicación exclusivo para esa transmisión. Ninguna otra información podía pasar por esa ruta mientras se estaba usando.

II.C. El Modelo de Interconexión de Sistemas Abiertos (*Open System Interconnection*)

El método de comunicación de paquetes se complementa con un modelo de interconexión de redes dividido en capas, conocido como Modelo de Interconexión de Sistemas Abiertos (MISA). El objetivo principal de MISA es estandarizar las funciones de un sistema de comunicación desde el cable que entra a nuestra casa hasta el ícono que aparece en la pantalla de la computa-

[12] Esta analogía también sirve para entender el concepto de manejo de tráfico. Los paquetes de datos viajan por diferentes direcciones, dependiendo de factores como el tamaño y el tipo. Los prestadores de servicios de Internet son, a la vez, los agentes de tránsito y quienes mueven el tráfico.

dora. El uso de las capas permite asignar funciones separadas y encadenadas una a otra: cada capa sirve a la de más arriba y ésta, a su vez, sirve a la siguiente. Usualmente, la capa superior cumple una función más compleja que la anterior.

«Estas capas forman una representación completa de la red, desde sus capacidades físicas (señales eléctricas enviadas a través de un cable o alambre telefónico, por ejemplo) en la capa uno, hasta las aplicaciones y servicios (correo electrónico, navegación, por ejemplo) en las capas más altas», explica Cooper.[13] Además de desagregar un complejo proceso y de facilitar la compatibilidad, MISA facilita la detección y manejo de errores en el sistema.

Gráfico. Capas de MISA y correspondencia con la conmutación de paquetes

Como muestra el gráfico, el encabezado y la carga útil de los paquetes de datos hacen parte de las capas más altas del modelo. El primero se relaciona con la capa de «transporte», mientras que la segunda abarca las de «sesión», «presentación» y «aplicación». En otras palabras, la carga útil –que, recordemos, incluye la «nuez» de la transmisión– está ubicada en las capas más altas, o profundas, del modelo. Al contrario, el encabezado está más próximo a la capa física, la más «superficial» de éste.

Examinemos este proceso con un ejemplo. Pablo le envía un correo electrónico a María a través de Gmail: esta acción está enmarcada en la capa de

[13] Cooper, A., «Doing de DPI Dance. Assessing the Privacy Impacto of Deep Packet Inspection», en *Privacy in America,* Scarecrow Press Inc., 2011, p. 149.

«aplicación», es decir, la más alta del modelo. El correo incluye el contenido (asunto y cuerpo del texto) y la dirección electrónica de María (maria@gmail.com), estos datos hacen parte de las capas «aplicación», «presentación» y «sesión», que son las que siguen en orden descendiente en el modelo y corresponden a la carga útil.

El mensaje también incluye datos sobre el orden de los paquetes y la aplicación o programa en que se ejecutan: éstos hacen parte de la capa de «transporte» y corresponden al encabezado. Por último, el mensaje sale de una dirección IP del computador de Pablo (215.33.57.120) dirigido a otra (en este caso, cualquier dirección IP del servidor de Gmail): estas coordenadas están en el tercer nivel –«red»– del modelo, que también hace parte del encabezado. Más abajo se encuentra el «enlace de datos», que es el cable que conecta la computadora a la red y, por último, la capa «física», donde está la conexión a Internet, cualquiera que esta sea. Cuando María reciba el correo en su cuenta, este proceso hará el recorrido inverso: de la capa «física» llegará a la de «aplicación», en la cual ella podrá leer el mensaje.

Para el objetivo de este documento no es necesario entender en detalle el funcionamiento de MISA. Lo importante es entender cómo se transporta la información en la red y cómo esta última se divide según las acciones jerarquizadas que se llevan a cabo y que se organizan en niveles. Y, concretamente para entender el monitoreo de contenidos, es relevante tener claro que en la medida en que un tercero quiera saber más sobre lo que hace una persona en Internet, mayor será el grado de inmersión en las capas. Para decirlo de manera coloquial: una cosa es leer los sobres de las cartas que le llegan al vecino y otra muy distinta es abrir los sobres y leer las cartas. A esto volveremos más adelante.

III. El deseo oficial de controlar Internet

El Principio de Extremo a Extremo y la conmutación de paquetes de datos son el sustento técnico de lo que se conoce en el debate público como «la neutralidad de la red» (*network neutrality*), término acuñado por el académico norteamericano Tim Wu, según el cual todos los contenidos en Internet reciben el mismo trato. La combinación de la «red tonta» con la transmisión de datos sin jerarquía alguna explican la innovación creciente y el intercambio de información –pluralista y democrático– que hoy conocemos.[14]

---

[14] Cfr. Wu, T., «Network Neutrality, Broadband and Discrimination», 2 *J. on Telecomm. & High Tech. L.,* 141, 2003.

No es necesario contar con una licencia para usar Internet de una manera específica (en la red, cualquiera puede ser bloguero o cantante), ni existe una única tecnología para difundir contenidos. A diferencia de la telefonía o de la televisión por cable, Internet es un sistema abierto y descentralizado. Sin embargo, estas características no están talladas en piedra; así como hoy en la red gozamos de innumerables puertas y ventanas, mañana podríamos tener una única entrada celosamente custodiada. Hoy nuestra interacción en la red se asemeja a jugar en un enorme patio; mañana podría parecerse más a jugar en la arenera de un parque.

Lessig considera que el usuario está sujeto a cuatro fuerzas que moldean su comportamiento en Internet: el mercado, que ofrece incentivos hacia el consumo de uno u otro producto; las normas sociales, que influyen en el comportamiento (por ejemplo, el reproche social hacia el uso de groserías en chats y redes sociales); la ley, que establece conductas punibles, y el código –la arquitectura de la red, los programas, los dispositivos–, que en última instancia define el entorno digital en el que nos movemos.[15]

«El código es ley en Internet», señala Lessig para subrayar el poder que el entorno digital tiene sobre el usuario. Por más que queramos, no podremos instalar Windows en un iPad o usar Facebook sin tener una cuenta registrada; por más que queramos navegar a una velocidad mayor, dependemos del servicio del proveedor de Internet.

La relación entre el código y la ley puede ser complementaria, principalmente cuando esta última resulta insuficiente para influir en la conducta de las personas. Mientras que una ley nacional que obligue a un usuario a suministrar su verdadera identidad en Facebook o Twitter tiene altas probabilidades de fracasar, un ley que imponga la obligación a los intermediarios tendrá un impacto inmediato. En el momento en que Facebook o Twitter exijan un número de identidad válido para iniciar sesión (que, por ejemplo, verificará contra una base de datos oficial), nuestro experiencia en la red habrá sido modificada.

Ese es, precisamente, uno de los pulsos más importante que vemos en la red: un esfuerzo por incrementar el control sobre el comportamiento de los usuarios en línea. Según Lessig, se trata de «cambios en la arquitectura de la

---

[15] Cfr. Lessig, L., *El Código Code 2.0,* edición en español, Traficante de Sueños, Madrid, 2009.

Red que permitirán mejorar el control estatal, al facilitar la vigilancia de las conductas –o al menos su rastreo–».[16]

Julie Cohen ofrece el término «arquitecturas de control», que responde al anhelo humano –más tradicional y mundano de lo que se cree– de «usar información y tecnologías de la información para manejar y estructurar el riesgo que se corre».[17]

Tal y como los «ciberlibertarios» temían, los Estados terminaron por reivindicar su soberanía nacional en el ciberespacio. Si bien la gobernanza de Internet en el contexto internacional está inmersa en un debate sin resolver sobre las instituciones que deben hacerse cargo y el origen que deben tener (desde la asignación de dominios de páginas hasta las decisiones sobre infraestructura), cada país ha optado por una estrategia previsible: regular la red dentro sus fronteras. Tendemos a creer que esta tentación solo existe en regímenes dictatoriales, pero la realidad es más tozuda.

> «A medida que Internet gana importancia y penetra más y más en los caminos de la vida pública, los gobiernos de Occidente están empezando a sentir –y muchos de ellos ya lo está sintiendo– una presión creciente para regularla. Parte de esta presión tendrá inevitablemente un origen ilegítimo, perjudicial y antidemocrático; mucha otra, no».[18]

Más allá del impacto que tengan, no todas las intervenciones de los gobiernos en la red son totalitarias. No es un asunto blanco o negro. El ejemplo de China, conocido por tener el cortafuegos o *firewall* más grande del mundo –que busca monitorear todo el contenido que entra y sale del país a través de Internet–, no resume el problema del control en Internet. A medida que se desarrolla la red, las zonas grises aumentan.

Los objetivos de intervención son tan amplios como las prioridades de cada país, más allá del sustento democrático que tengan. Algunos Estados de Medio Oriente, por ejemplo, consideran inaceptable que se difunda pornografía a través de Internet; otros, como Estados Unidos, priorizan la lucha contra el terrorismo, y algunos más, como Alemania, quieren prevenir que ciertos discursos políticos –palabras, imágenes– exacerben el doloroso pasado. En

---

[16] *Ibíd*em, p. 231.

[17] Cohen, J., *Configuring the Networked Self,* Yale University Press, Londres, 2012, p. 156.

[18] Mozorov, E., *The Net Delusion,* Public Affairs Books, Nueva York, 2011, p. 218.

un sentido similar, el proyecto de ley argentino (1892 de 2012), que en buena medida anima este documento, pretende «detectar, combatir y denunciar» expresiones de acoso, discriminación y violencia en Internet. La pregunta que se desprende es: ¿cómo se hace?

III.A. Los guardianes: la llave del control

Algunos Estados controlan el uso de Internet –de manera directa y permanente– a través de un brazo burocrático, auténticos ejércitos dedicados a monitorear la actividad en línea. Para hacerlo, emplean estrategias como la intervención en los Servidores Raíz de Nombre de Dominio, que relacionan las direcciones IP con los sitios de Internet, o en la espina dorsal de la red, que conecta los puntos críticos del tráfico de datos.

En términos prácticos, esto implica que el gobierno puede «apagar» Internet como si fuera un interruptor de luz. En diferentes grados, y dependiendo del músculo oficial, éste es el caso de países como Arabia Saudita, China y Cuba.[19] A esto se suma el uso de la Inspección Profunda de Paquete, de la que hablaremos más adelante.

La mayoría de países opta por una estrategia acaso más sencilla y eficiente (aunque no excluyente con la anterior): acudir a los intermediarios –los Prestadores de Servicios de Internet y los Operadores de Servicios en Línea (PSI y OSL, respectivamente)– que hacen las veces de «guardianes» (*gatekeepers*) de la red. Un guardián es un agente que ocupa una posición privilegiada, controla el acceso a un sitio o el uso de un recurso: del PSI depende nuestro acceso a Internet, y de aplicaciones y servicios como Google, Facebook, o de «nubes» como Dropbox (todos ejemplos de OSL) depende en gran medida nuestra experiencia en línea. Tal protagonismo es útil para los gobiernos, que encuentran en estos terceros un aliado –voluntario u obligado– para sus propósitos.

El uso de estos intermediarios para aplicar la ley no es una teoría nueva. Cuando existen conductas que las normas no logran desestimular (por ejemplo, una sanción penal para frenar la piratería en línea), cuando el Estado se encuentra en una posición desventajosa para hacerlas cumplir y cuando hay un intermediario en una posición privilegiada para detenerlas, el uso de incen-

---

[19] Cfr. Zittrain, J. y Palfrey, J., «Internet Filtering: The Politics and Mechanisms of Control», en *Acces Denied,* The MIT Press, 2008; y Freedom House, *Freedom on the Net 2011,* Washington, 2011.

tivos –legales, económicos– permite que este último ayude a cumplir los fines que escapan a la órbita oficial.[20]

En otras palabras, en muchos casos la oferta de los gobiernos hacia estas empresas ha sido: «o nos ayudan a detectar ciertos contenidos o ustedes también serán responsables». Esta estrategia ha ganado terreno en la gobernanza de Internet mediante la creación de «puertos seguros» (*safe harbors*) para los intermediarios, con las consecuencias negativas para el uso abierto de la red y la afectación de los derechos individuales.[21]

Tanto los gobiernos como los intermediarios (de manera independiente o conjunta) se valen de sofisticados equipos y servicios ofrecidos por empresas británicas o norteamericanas, entra muchas otras, para monitorear la red.[22] En particular, el mercado está inundado de productos para hacer Inspección Profunda de Paquete.

Recientemente, cuando se conoció que el gobierno sirio usaba esta tecnología para perseguir disidentes, e incluso la habría usado para ubicar a la periodista Marie Colvin –que posteriormente murió en un bombardeo junto con un fotógrafo francés–, varias organizaciones de la sociedad civil protestaron.[23] Sin embargo, su uso es más generalizado y, como planteábamos al comienzo del capítulo, es parte de diferentes estrategias de los gobiernos para ejercer su soberanía en Internet.

III.B. La inspección: de superficial a compleja

Desde el punto de vista técnico, la manera de ejercer el control es la parte más complicada. Si tenemos claro el funcionamiento básico de Internet

---

20 Cfr. Kraakman, R., «Gatekeepers: The Anatomy of a Third Party Enforcement», *Journal of Law, Economics and Organization,* Vol. 2, Nº 1, 1986.

21 El «puerto seguro» ofrece al intermediario la garantía de no ser responsable por las acciones de sus usuarios, siempre y cuando cumpla con ciertas actuaciones. Este tema se aborda parcialmente en el artículo *La tensión entre la propiedad intelectual y el intercambio de contenidos en la red,* en esta misma obra.

22 Ver «Selling arms and snooping technology is no way to help democracy, Cameron», Privacy International, disponible en: http://www.privacyinternational.org/opinionpieces/sellingarmsandsnoopingtechnologyisnowaytohelpdemocracycameron (consultada el 19 de junio de 2012).

23 Ver Galperin, E., «Don't get your sources killed in Syria», Comittee to Protect Journalists, disponible en: https://www.cpj.org/security/2012/05/dontgetyoursourcesinsyriakilled.php (consultada el 19 de junio de 2012).

(expuesto antes) podemos vislumbrar lo complejo que es monitorear sus contenidos. No hay un programa o dispositivo que de manera automática detecte y retire de la red aquello que puede ser perjudicial o inconveniente; no existe un procedimiento aséptico y quirúrgico. Al contrario, es necesario desplegar tecnologías que intervienen la red, de las cuales la Inspección Profunda de Paquete o *Deep Packet Inspection* (IPP) es una de las más importantes, especialmente cuando se trata de monitorear contenidos en Internet.[24]

Retomemos el ejemplo del capítulo anterior en el que Pablo envía un correo electrónico a María. Cada función se ubica en una capa diferente, desde la más alta (el uso de la aplicación para producir y enviar el mensaje) hasta la más baja (los cables que transportan los datos). Así, la cantidad de información disponible sobre los datos de esta transmisión dependerá de qué capas estemos observando. Por ejemplo, si observamos la capa «red» –en el tercer nivel–, tendremos acceso a la dirección IP del computador tanto de Pedro como de María; si profundizamos un poco más, hasta la capa «transporte» –en el cuarto nivel–, sabremos que los datos corresponden a Gmail o Google, y si llegamos hasta la «sesión» y «presentación» –en los últimos niveles–, sabremos qué dice el correo electrónico.

Para observar o acceder a esos datos es necesario inspeccionar los paquetes. Esto es, revisarlos mientras pasan por un punto de la red, de la misma manera como se abren o inspeccionan con un escáner las maletas en un aeropuerto. Y para hacerlo, se requieren dispositivos y programas especiales que –con diferentes grados de precisión y sofisticación– puedan hacer ese trabajo en una o varias de las capas, a través de la IPP.

El dispositivo, conocido también como «caja negra», debe estar conectado a la red para poder observar el tráfico. Puede estar en la red de los PSI o de los OSL, en los enrutadores de las entidades públicas o en las espinas dorsales de la red. La capacidad técnica varía según el producto: un tipo de IPP puede copiar algunos de los paquetes para inspeccionarlos posteriormente o simplemente observarlos mientras transitan por la red. Lo cierto es que «entre más cerca llega una tecnología de inspección a supervisar la capa de aplicación de la carga útil, más podrá saber esta tecnología sobre el paquete».[25]

Según Cooper, la IPP «es la colección, observación, análisis y/o almacenamiento de datos relacionados con una aplicación que se encuentra en Internet

---

[24] Existen muchas otros tipos de intervención, como el filtrado de encabezados o la manipulación del Sistema de Nombres de Dominio.

[25] Parsons, *supra* nota 10, p. 3. Traducción informal.

por encima de la capa tres»,[26] es decir, de la capa de «transporte» en adelante. Parsons, mientras tanto, define la IPP al ubicarla en el nivel más radical de una escala de tipos de inspección:[27]

i) Inspección Superficial de Paquete: incluye los «cortafuegos» –o *firewalls*– que tienen sistemas operativos como Windows o Apple OS X, y que se ubican entre el cliente y la red a la que éste está conectado. El objetivo de esta inspección es limitar que cierto tipo de contenido, determinado por el usuario, llegue o abandone el equipo. Sin embargo, para hacerlo no puedo leer más allá del encabezado de los paquetes. Esto es, no puede revisar la carga útil.

ii) Inspección Media de Paquete: referida normalmente a los dispositivos ubicados entre el usuario final y la compuerta a Internet o salida al PSI (conocidos como *proxys*). Este tipo de controles son normales en entidades públicas y empresas privadas: todo el tráfico que pasa sobre la red debe cumplir con las reglas impuestas por el administrador, como bloquear el acceso a YouTube o a Facebook para los empleados. En términos de inspección –explica Parsons–, este tipo de inspección puede leer la capa de «presentación», con lo cual accede parcialmente a la carga útil de los paquetes. En otras palabras, es la antesala de la IPP.

iii) Inspección Profunda de Paquete (IPP): Parsons coincide con la definición de Cooper en cuanto a que los dispositivos en esta categoría tienen el potencial de mirar todo el tráfico, escoger paquetes y rearmarlos para conocer los datos objeto de la transmisión. Volviendo al ejemplo de Pedro y María, esta tecnología puede reconstruir el correo tal y como fue escrito.[28]

Existen procesos de inspección y manejo de paquetes esenciales para el funcionamiento de la red, lo cual es natural en cualquier sistema de comunicación. Cooper considera que para intermediarios como los PSI el uso de la IPP «puede ofrecer una mayor comprensión sobre cómo están siendo usadas sus redes, permitiéndoles tomar decisiones más informadas sobre actualizaciones de la red y arquitectura de ésta».[29]

---

[26] Cooper, *supra* nota 13, p. 145. Traducción informal.

[27] Cfr. Parsons, *supra* nota 10, ps. 8 y ss.

[28] Existen tecnologías de encriptación de paquetes para combatir el uso de IPP. Para muchos, éste puede ser el «antídoto» del monitoreo de contenidos. No obstante, su uso está restringido –tanto por razones técnicas como económicas– a ciertas aplicaciones y sectores.

[29] Cooper, *supra* nota 13, p. 140. Traducción informal.

Si enviamos una carta por el servicio postal físico, la empresa de correos tendrá que saber cuál es la dirección de remisión y envío y, posiblemente, también el contenido general del sobre o su peso. De la misma manera, en la relación entre el emisario y el receptor en Internet hay, al menos, un tercero que tiene acceso a cierta información de la transmisión.

Adicionalmente, es innegable el incentivo económico que tienen los intermediarios para hacer esto. El uso de la IPP le ha permitido a algunos PSI discriminar el tráfico de sus usuarios con el propósito de manejar su mercado (volviendo a la analogía de la autopista, la IPP sirve para crear carriles rápidos, de automóviles último modelo, y lentos, de camiones y autos viejos). Así, utilizan los datos de los encabezados IP para enrutar los paquetes que envían y reciben sus suscriptores, e inspeccionan los encabezados TCP –muchas veces de manera poco transparente– para tener alguna información adicional sobre la actividad de éstos.

Por ejemplo, a un PSI le interesa saber que uno de sus usuarios descarga películas o intercambia archivos de gran tamaño en redes de pares (*peer to peer networks* o P2P). Basado en esto, puede optar por restringir la descarga en ciertos horarios o manejar el tráfico para evitar congestiones en la red. En 2010, el PSI norteamericano Comcast estuvo involucrado en, al menos, un caso de este tipo.[30] Aunque el asunto del monitoreo de contenidos como parte de una estrategia comercial y económica es muy relevante, este documento no lo desarrolla por no estar dentro del enfoque propuesto. No obstante, para muchos observadores se trata de una estrategia que atenta contra la esencia de la neutralidad de la red.

Más allá del negocio y de los argumentos técnicos, el problema surge cuando la labor de inspección se mueve del rango de los simples encabezados de los paquetes, esenciales para prestar el servicio o garantizar la seguridad del sistema, hacia la carga útil de los mensajes; cuando combinando y sumando información, el tercero comienza a acceder a datos sensibles del usuario o a perfilarlo a partir de sus actividades en la red. Y, más relevante aún, el problema surge cuando los gobiernos promueven o están al tanto del uso de estas tecnologías en detrimento (y a espaldas) de los usuarios.

---

30 Ver «Appeals Court Throttles FCC's Net Neutrality Authority», Wired, disponible en: http://www.wired.com/threatlevel/2010/04/netneutralitythrottle/ (consultada el 19 de junio de 2012).

IV. El monitoreo en la balanza

Si sostenemos –como lo venimos haciendo– que resulta apresurado concluir que cualquier intención oficial de monitorear la red es sinónimo de represión, tenemos que preguntarnos, entonces, en qué medida esa intervención es legítima y ajustada a principios democráticos. Y, para hacerlo, es necesario repasar los fines que persiguen los gobiernos al ejercer su soberanía en Internet.

En general, esta intervención se sustenta en los bienes comunes de la seguridad nacional y el orden público, y en la necesidad de establecer límites a la libertad de expresión. Todos estos valores están enmarcados en garantías reconocidas tanto en constituciones nacionales como en instrumentos de derecho internacional. A continuación ofreceremos algunos ejemplos para, posteriormente, hacer un análisis crítico.

IV.A. La necesidad de una red segura

Tener algún tipo de acceso a la información que se intercambia en cualquier sistema de comunicación ha sido una obsesión permanente de las agencias de inteligencia y la fuerza pública en todo el mundo. Para el juez norteamericano Richard Posner, «en una era de terrorismo global y proliferación de armas de destrucción masiva, el gobierno tiene la imperiosa necesidad de recoger, extraer, depurar y buscar vastas cantidades de información».[31]

La necesidad de combatir el terrorismo y el crimen y, en general, de recabar pruebas judiciales, son objetivos de primer orden, aun a costa de la libertad e intimidad de los ciudadanos. Una agenda que, sin duda, ganó terreno a partir del atentado terrorista del 11 de septiembre de 2001 en Estados Unidos. En palabras de Naomi Klein, después de los ataques, «de repente el miedo al terror era mucho mayor que el miedo a vivir en una sociedad vigilada».[32]

Este objetivo no es nuevo. En 1994, el Congreso norteamericano expidió la ley Calea (*Communications Assistance for Law Enforcement*), según la cual las redes de telecomunicaciones deben diseñarse para que las agencias de seguridad puedan llevar a cabo una vigilancia electrónica. La regulación esta-

---

[31] Posner, R., en Solove, D., *Understanding Privacy*, Harvard University Press, Londres, 2008, p. 83. Traducción informal.

[32] Klein, N., *Shock Doctrine,* Picador, Nueva York, 2007, p. 382. Traducción informal.

ba pensada para el teléfono –una tecnología más fácil de monitorear–, pero su aplicación se ha hecho extensiva a Internet y, particularmente, a los PSI.[33]

Hoy en día, conscientes del poder de los guardianes en Internet, el FBI está promoviendo una ley que extienda esta obligación a los OSL. Es decir, para que Facebook o Twitter, por ejemplo, tengan también una «puerta de atrás» (*backdoor*), por donde pueda entrar el gobierno a mirar cuando sea necesario.[34]

El Reino Unido está inmerso en un debate similar. En 2009, el gobierno laborista propuso que los PSI registraran todas las transmisiones de datos de los usuarios de Internet mediante el uso de «cajas negras» de IPP. Recientemente, la propuesta se retomó con el Programa de Desarrollo de las Capacidades de Comunicación (*Communications Capabilities Development Programme*), que incluye a los OSL.

Si bien el gobierno inglés ya contaba con herramientas para solicitarle a los intermediarios información de sus usuarios que tuvieran almacenada (en virtud del Acto para la Regulación de Poderes de Investigación de 2000), esta propuesta permitiría monitorear y detectar contenidos permanentemente. En el momento en que este documento se publicó, el texto definitivo del proyecto apenas comenzaba a conocerse.[35]

El antecedente inmediato de esta propuesta son los disturbios en Londres del año pasado. Como parte de la respuesta oficial, el primer ministro inglés David Cameron manifestó que su gobierno estaba explorando maneras de prohibir el uso de redes sociales cuando hubiera indicios de que serían usadas para organizar actividades criminales.[36]

---

[33] Cfr. Lessig, *supra* nota 15, ps. 63 y ss.

[34] Ver «FBI: We need wiretapready Web», CNet, disponible en: http://news.cnet.com/83011009_35742806783/fbiweneedwiretapreadywebsitesnow/ (consultada el 19 de junio de 2012).

[35] Ver «Draft Communications Bill reveals Home Office's mass surveillance plans going ahead but government remains tonguetied about how technology will actually work», Privacy International, disponible en: https://www.privacyinternational.org/pressreleases/draftcommunicationsbillrevealshomeofficesmasssurveillanceplansgoingahead (consultada el 19 de junio de 2012).

[36] Ver «United Kingdom: David Cameron Considers Banning Rioters from Social Media, Index on Censorship», disponible en: http://www.indexoncensorship.org/2011/08/unitedkingdomdavidcameronconsidersbanningriotersfromsocialmedia/ (consultada el 19 de junio de 2012).

En el mismo sentido, en marzo de este año, el entonces presidente francés Nicolás Sarkozy propuso, como reacción a los asesinatos en Tolouse por parte de un extremista islámico, que se tramitara una ley para encarcelar a las personas que visitan constantemente sitios que «promueven el terror» en Internet.[37]

América Latina no es ajena a esta tendencia. En 2010, en México, el Partido de la Revolución Democrática presentó un proyecto de ley para monitorear y reglamentar el uso de redes sociales. El objetivo principal era prevenir la actividad en línea de los carteles del narcotráfico, que usan las redes sociales para intercambiar información sobre crímenes. Adicionalmente, existe la preocupación de que algunos blogs y sitios de Internet se usan para incitar a la violencia y hacer apologías del crimen organizado. Hasta el momento no se conocen avances de la iniciativa.[38]

En este enfoque cae también uno de los proyectos de ley argentinos mencionados en la introducción (1892 de 2012), cuyo objetivo es: «detectar, combatir y denunciar las prácticas denominadas como ciber acoso o *ciberbullyng*, preservar el ámbito de Internet de cualquier tipo de manifestación de violencia que afecte los derechos de grupo, comunidades o personas y cualquier otra práctica de contenido y/o carácter discriminatorio». Añade la exposición de motivos que «defender la libertad de las plataformas digitales es defender que todos sean igual de libres para expresarse sin ser agredidos o discriminados».

Una última aproximación, tal vez menos relevante en nuestra región, se refiere al interés de algunos Estados de hacer cumplir en Internet la religión que profesan. Arabia Saudita, por ejemplo, emplea sistemas de monitoreo y filtrado para evitar el acceso a sitios que menoscaben el culto o que vayan en contra de sus preceptos.[39]

---

[37] Ver «Sarkozy propone encarcelar a quien frecuente sitios web terroristas», *Infobae.com*, disponible en: http://america.infobae.com/notas/46914Sarkozyproponeencar celaraquienfrecuentesitioswebterroristas (consultada el 19 de junio de 2012).

[38] Cfr. Ferraz, J. *et al.*, «Filtrado de contenido en América Latina: razones e impacto en la libertad de expresión», en *Hacia una Internet libre de censura. Propuestas para América Latina,* Centro de Estudios en Libertad de Expresión y Acceso a la Información, Facultad de Derecho, Universidad de Palermo, 2012, ps. 182 y ss.

[39] Cfr. Nunziato, Dawn C., «Preservar la libertad en Internet en las Américas», en *Hacia una Internet libre de censura. Propuestas para América Latina,* Centro de Estudios en Libertad de Expresión y Acceso a la Información, Facultad de Derecho, Universidad de Palermo, 2012, ps. 25 y ss.

Esta es apenas una muestra del interés de los Estados de hacer valer principios que, a primera vista, conviven en nivel de importancia con la libertad de expresión. Según Zittrain y Palfrey, para los Estados, «la libertad de expresión nunca ha sido absoluta, incluso en aquellas democracias liberales que valoran estas libertades más encarecidamente».[40] Y si así ha sido siempre, ¿por qué habrá de ser diferente en Internet?

IV.B. Privacidad, vigilancia y libertad de expresión

El monitoreo de contenidos en Internet reduce la órbita de privacidad del individuo, modifica su interacción con la red y condiciona su libertad de expresión. Esta afectación subsiste más allá de la finalidad del monitoreo o, incluso, así no exista una en particular. Tal impacto parte del supuesto de que el individuo sabe o sospecha que su actividad en línea está siendo monitoreada. Si se lleva a cabo sin su conocimiento, la situación sería aún peor, ya que no se le estaría reconociendo siquiera la titularidad de sus derechos más elementales.

El monitoreo en línea constituye una forma de vigilancia, y su penetración en la vida de las personas aumenta en la medida en que las relaciones sociales, laborales y económicas están cada vez más mediadas por el uso de Internet. Hace 20 años, poco o nada podía saberse de una persona al observar su actividad en la red; hoy en día puede tenerse una radiografía exacta.

Muchos autores se refieren al impacto que la vigilancia tiene en el individuo. La observación permanente busca controlar y normalizar las conductas de la persona, que opta por actuar de conformidad con la expectativa –explícita o implícita– de quien lo observa. Consciente de que está siendo monitoreada, la persona inhibe su espontaneidad y evita cualquier clase de experimentación.[41] De hecho, volver un espacio predecible y controlable es uno de los objetivos de sistemas como los circuitos cerrados de televisión en lugares públicos (estaciones de metro, parques y calles).

El monitoreo de las actividades en línea es también una violación a la privacidad. Es posible argumentar que una persona no tiene una expectativa de

---

[40] Zittrain y Palfrey, *supra* nota 19, ps. 31 y 32.

[41] Foucault, M., en Reiman, J., «Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future», *Santa Clara Computer & High Technology Law Journal,* Vol. 11, Nº 1, 1995, p. 28. Traducción informal.

privacidad en un parque, pero no podría decirse lo mismo de su casa, su lugar de trabajo o su computadora. «Una invasión a la privacidad interfiere con la integridad de ciertas actividades e incluso destruye o inhibe algunas de ellas», afirma Solove.[42]

La afectación de la privacidad no se limita únicamente al hecho de que un tercero esté al tanto de asuntos de un individuo que este último quisiera que no se supieran; la ausencia de privacidad afecta también el proceso de subjetividad de la persona y la relación de ésta con su entorno. Según Cohen, la construcción de la identidad es también un proceso de prueba y error, de juego y ensayo.[43]

Usemos, nuevamente, un ejemplo: Internet es una entrada para la exploración de temas, contenidos e interacciones de todo tipo. Una persona puede estar interesada en la historia de la guerrilla en América Latina, y con ese propósito busca videos y textos, intercambia mensajes y transmite opiniones. Esta actividad no se relaciona con su vida personal ni se basa en algún deseo de ingresar a un grupo armado ilegal. Hace parte de una manifestación espontánea (estudiar Historia, entender los movimientos sociales), que puede potenciarse gracias a la reclusión que le ofrece Internet. No obstante, ante un monitoreo de estas actividades, o un indicio de que está sucediendo, esta persona optará por restringir este aspecto de su individualidad.

El costo para la libertad de expresión es evidente. Un individuo que no goza de un espacio para reflexionar, pensar y formar su criterio, no podrá manifestarse de manera libre. «Los efectos de esta pérdida de confianza podrían ser de amplio alcance. Así como con otras tecnologías de vigilancia, el uso creciente de la IPP crea el potencial para la autocensura e inhibición en línea».[44]

IV.C. Garantías fundamentales e incentivos perversos

El último punto que deseamos plantear se refiere, por un lado, a la manera como los gobiernos implementan las políticas de monitoreo y, por el otro, a los incentivos que generan. Y tal vez acá está el mayor síntoma de preocupación: llama la atención que los gobiernos quieran vigilar Internet, pero llama la atención sobre todo la manera como lo ponen en práctica.

---

42 Solove, *supra* nota 31, p. 9.

43 Cfr. Cohen, *supra* nota 17.

44 Cooper, *supra* nota 13, p. 147.

Las declaraciones de Cameron y Sarkozy y los proyectos de ley en Argentina y México referidos tienen un común denominador: ponerlos en práctica implicaría el uso de mecanismos como la IPP. Si el objetivo es detectar palabras, datos e informaciones que se intercambian en la red permanentemente, la única manera de hacerlo es a través de tecnologías intrusas como esa. No existe, al menos hasta ahora, un proceso aséptico para monitorear Internet.

Surgen entonces varias preguntas: ¿cuál sería la fuente de estas medidas, una decisión administrativa, una ley o una decisión judicial?, ¿se hará en desarrollo de controles previos o posteriores?, ¿qué tipo de recursos tendrían los ciudadanos para apelar, o al menos conocer, las decisiones sobre el monitoreo de su actividad en línea?

Hablar de regulación de Internet requiere, como hemos visto, de un conocimiento técnico. Sin embargo, las preguntas planteadas se relacionan con garantías reconocidas por legislaciones nacionales y tratados internacionales, cuya aplicación no debe ser ajena al ámbito de Internet. De la misma manera como los gobiernos reclaman su soberanía en este espacio, es necesario reivindicar la vigencia de estos instrumentos en la era digital.

Aquí no describiremos el marco legal que aplica en este asunto. Baste con señalar que resulta imprescindible analizar las políticas de monitoreo en línea y, específicamente, el uso de tecnologías como la IPP, a la luz de derechos reconocidos en la Convención Interamericana sobre Derechos Humanos como el de las garantías judiciales (artículo 8), la honra y la dignidad (artículo 11), y la libertad de pensamiento y expresión (artículo 13).

En relación con este último, la Declaración conjunta acerca de Internet, de junio de 2011, de los relatores de libertad de expresión de las Naciones Unidas y de la Comisión Interamericana de Derechos Humanos, y la representante de la Organización para la Seguridad y la Cooperación en Europa, manifestaron lo siguiente:

> «La libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación. Las restricciones a la libertad de expresión en Internet solo resultan aceptables cuando cumplen con los estándares internacionales que disponen, entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad (la prueba “tripartita”)».[45]

45 Relatoría Especial para la Libertad de Expresión, comunicado de prensa R50/11, disponible en: http://cidh.org/relatoria/showarticle.asp?artID=848&lID=2 (consultada el 19 de junio de 2012).

Por supuesto, sería excesivo argumentar que las autoridades judiciales y de inteligencia no deben tener ninguna clase de herramientas para monitorear la actividad en Internet de una persona. Estas prerrogativas deben existir, pero sus límites deben estar claramente establecidos. En términos prácticos, pueden aplicarse los criterios existentes para la retención de datos o para la interceptación tradicional de comunicaciones.[46] En la misma dirección apunta la prueba «tripartita» de la que hablan los Relatores. Esto es, debe haber, al menos, proporcionalidad en la actuación, legalidad y control judicial.

Con este contexto en mente, la idea de un observatorio de redes sociales –como un órgano del Ejecutivo o como un cuerpo mixto–, en los términos en que propone el proyecto de ley argentino, puede convertirse en un instancia arbitraria de vigilancia. No sólo los ciudadanos desconocerían los términos en que tal monitoreo se llevaría a cabo, sino que también carecerían de acciones judiciales para cuestionarlo.

«La mayoría de la regulación que autoriza a las agencia estatales a llevar a cabo filtrado y vigilancia tiende a estar escrita en términos amplios y vagos»,[47] argumentan Zittrain y Palfrey. En este punto coincide Nunziato.[48] Estas ambigüedades legales, que son problemáticas en sí mismas, son aún más riesgosas aplicadas a asuntos de tecnología. En el caso inglés, por ejemplo, las autoridades han dicho en su defensa que el uso de la IPP se limitará a obtener ciertos datos de la comunicación (como saber si una persona le envió un mensaje a otra), sin mirar el contenido. Lo cierto es que obtener esos datos de la comunicación implica técnicamente, en muchos casos, tener acceso a su contenido.

El discurso oficial también termina por convertirse en un incentivo perverso para los intermediarios de Internet, sin mencionar los incentivos económicos ya existentes. El riesgo de terminar respondiendo legalmente por las conductas de sus usuarios, lleva a los PSI y OSL a monitorear cada vez más a sus

---

[46] En la región ya existe regulación especial para la materia. La ley 1273 de 2009 de Colombia, por ejemplo, incluye el delito de interceptación sin autorización de datos informáticos: «El que sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses».

[47] Zittrain y Palfrey, *supra* nota 19, p. 33.

[48] Cfr. Nunziato, *supra* nota 39, ps. 11 y ss.

abonados, incluso desbordando el límite de la relación contractual entre las partes. Todo lo cual sucede mientras el ciudadano navega por Internet de manera desprevenida.

Resulta prioritario entender el impacto que tienen las propuestas y discursos oficiales en la regulación de Internet. Llevada a la práctica, la idea de monitorear y detectar contenidos en línea pone en riesgo las garantías fundamentales de los ciudadanos y amenaza con desmontar el entorno digital abierto y pluralista que conocemos. Adicionalmente, estas iniciativas deben darse de manera abierta y transparente, bajo la premisa de que los debates tecnológicos –cualquiera que sea su nivel de complejidad– deben estar al alcance de la sociedad y de las instituciones democráticas.

V. Recomendaciones

A manera de cierre, y sin excluir otros puntos que hemos señalado en el texto, hacemos las siguientes recomendaciones:

• Necesidad de amplia participación y consulta: las discusiones de proyectos de ley sobre monitoreo de contenidos en Internet que se lleven a cabo deben contar con una participación amplia, que garantice la inclusión de todos los puntos de vista y un adecuado nivel de conocimiento sobre los temas técnicos.

• Necesidad de estudios de impacto a derechos humanos: en relación con la recomendación anterior, sugerimos que los proyectos de ley que buscan establecer mecanismos de monitoreo de contenidos en Internet cuenten con un estudio técnico previo sobre el impacto que tendrían en materia de derechos humanos y en la arquitectura de la red. Los resultados de éste deben explicitarse en la exposición de motivos de la iniciativa.

• Necesidad de transparencia e información de los PSI y OSL: los Proveedores de Servicios de Internet y los Operadores de Servicios en Línea deben informarles a sus usuarios cómo y en qué condiciones monitorean sus contenidos. Esta obligación incluye el uso de tecnologías como la Inspección Profunda de Paquete.

• Transparencia e información de los gobiernos: los gobiernos deben hacer explícitas las políticas de vigilancia y monitoreo de Internet, bien sea en desarrollo de leyes existentes o de decisiones administrativas. Específicamente, deben ser transparentes con las obligaciones que imponen a los intermediarios.

• Necesidad de delimitar el uso de herramientas de monitoreo: las autoridades judiciales y de inteligencia pueden contar con herramientas legales para monitorear la actividad en línea de los ciudadanos. Sin embargo, éstas deben

estar sujetas a las mismas restricciones que se aplican en otros temas, como la protección de datos y la interceptación de comunicaciones.

• Necesidad de ampliar el debate con los usuarios: las organizaciones de la sociedad civil que trabajan en estos temas deben hacer un esfuerzos por acercar a los usuarios a este debate. Esto incluye la formación en herramientas legales y derechos humanos aplicadas a Internet.

Las llaves del ama de llaves: la estrategia de los intermediarios en Internet y el impacto en el entorno digital[1]

Resumen

El objetivo de este documento es ofrecer un sustento teórico y un contexto mínimo para el debate sobre la responsabilidad de los intermediarios en Internet con énfasis en los problemas relacionados con contenidos.

El primer apartado explica el fundamento teórico general sobre los intermediarios y su relación con la responsabilidad civil. Allí se analiza la importancia del balance entre los costos que asume el intermediario y los beneficios que obtiene por ejercer su rol de guardián.

Posteriormente se describen los antecedentes que llevaron a los intermediarios en Internet a convertirse en guardianes de los usuarios. Una vez desmontado el argumento de la imposibilidad tecnológica –explica el documento– quedó claro que el Prestador de Servicios de Internet estaba llamado a ejercer el rol de guardián de los usuarios.

El tercer apartado se refiere a los tipos de guardianes y sus deberes, haciendo énfasis en los modelos más comunes. Ninguna de las leyes sobre responsabilidad de intermediarios ha establecido un régimen de responsabilidad objetiva. Las leyes varían entre lo que se conoce como una inmunidad total o una inmunidad condicionada.

---

[1] Este documento fue elaborado por Carlos Cortés Castillo, investigador de la Iniciativa por la Libertad de Expresión en Internet (iLEI), del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo. La investigación y elaboración del documento fue dirigida y contó con los comentarios de Eduardo Bertoni, director del CELE.

En seguida se hace un breve análisis de lo que se avizora en el horizonte en este tema. Algunos autores consideran que en el futuro los intermediarios usarán cada vez más el filtrado de contenidos como estrategia para ejercer su papel como guardianes. Y siguiendo la idea de que así como la tecnología puede restringir el entorno digital lo puede fortalecer, se recomienda explorar soluciones tecnológicas para equilibrar el debate en Internet.

Por último, y a partir de lo expuesto, el documento hace las siguientes recomendaciones:

• Es importante considerar el balance entre los costos que asume el intermediario y los beneficios que obtiene por ejercer su rol de ama de llaves. Un desequilibrio entre éstos implica una estrategia fallida que además impacta negativamente en actividades socialmente deseables y afecta derechos fundamentales como el debido proceso y la libertad de expresión.

• Establecer un régimen de responsabilidad objetiva para los intermediarios de Internet resulta inadecuado. Por un lado, implica imponerle obligaciones difusas a éstos, más allá de las que realmente podrían cumplir. Por el otro, se traduciría en mayores restricciones para los usuarios de Internet, en contravía de derechos y garantías fundamentales. Las decisiones judiciales en Argentina ilustran el problema de que el intermediario esté obligado a hacer juicios de valor sobre la legalidad de las acciones del usuario.

• La inmunidad condicionada parece adecuada como régimen de responsabilidad cuando establece incentivos razonables para el guardián. Es decir, cuando no le impone deberes difusos o desproporcionados de monitoreo y vigilancia. Sin embargo, en algunos modelos de inmunidad condicionada –como el del DMCA de Estados Unidos– los costos que no asume el intermediario terminan en cabeza de los usuarios y la comunidad en general. En este caso los costos son vulneraciones a derechos como la libertad de expresión y el debido proceso.

• En esos términos, y sin subestimar el problema del contenido agresivo y difamatorio que pulula en la red, una inmunidad condicionada en materia de responsabilidad de intermediarios por contenidos de sus usuarios podría implicar, en la práctica, la derogación de la libertad de expresión y el debido proceso en Internet.

• Los debates sobre la responsabilidad de los intermediarios deben prestarle atención a la práctica del filtrado de contenidos, que aparece en el horizonte como una estrategia invisible para que el amo de llaves ejerza la guardia. Esto implica, de paso, empezar a mirar las condiciones que acepta el usuario cuando adhiere a los términos de referencia del servicio.

• Vale la pena explorar la idea de implementar soluciones tecnológicas –en todas sus versiones– para enfrentar los contenidos difamatorios que abundan en Internet. Particularmente, es posible pensar en adaptar un derecho de réplica a diferentes tipos de servicios y plataformas.

I. Introducción

En un día cualquiera frente a la computadora usamos, al menos, dos servicios que nos presta alguna empresa –nacional o extranjera–: el de la conexión a la red y el del correo electrónico. Pero por supuesto el número es mayor: entramos a algún portal de información, miramos las actualizaciones en Facebook, recomendamos un artículo por Twitter, buscamos información en Google, comentamos un blog, miramos libros en Amazon, oímos música en Spotify o Lastfm… La lista es interminable.

Estas empresas –los intermediarios– no solo hacen posible nuestra actividad en línea sino que también la moldean. Para algunos servicios necesitamos clave, para otros debemos pagar, en algunos podemos escribir extensamente, en otros solo unas cuantas palabras. De manera creciente el espacio abre más posibilidades y a la vez está sujeto a mayores reglas y obstáculos.

A medida que esa vida digital se expande, tanto el Estado como las empresas incrementan su interés por controlar nuestra actividad en línea y prevenir hechos indeseados. Los contextos sociales se trasladan a Internet. Algunos problemas, como la piratería, parecen magnificados y otros, como la pornografía infantil, revisten gravedad.

En medio de esta situación de evolución y cambio, de tensiones y agendas opuestas, los Estados vienen diseñando fórmulas para que los intermediarios en Internet respondan por los posibles delitos cometidos por sus usuarios. Y en medio de esa agenda de regulación y órdenes judiciales, derechos como la libertad de expresión o el debido proceso parecen quedar en paréntesis.

El objetivo de este documento es ofrecer un sustento teórico y un contexto mínimo para el debate sobre la responsabilidad de los intermediarios en Internet con énfasis en los problemas relacionados con contenidos. Con esa idea en mente, no encontrarán acá un estudio comparativo de los regímenes existentes ni un análisis meramente jurídico. El objetivo es trazar puentes disciplinarios y abstraer los elementos más relevantes del tema para identificar problemas y ofrecer algunos puntos de análisis.

El documento está divido de la siguiente manera: el primer capítulo explica el fundamento teórico sobre los intermediarios y su relación con la responsabilidad civil; el segundo describe los antecedentes generales que llevaron a

los intermediarios en Internet a convertirse en guardianes de los usuarios; el tercero explica los tipos de guardianes y sus deberes, haciendo énfasis en los modelos más comunes; el cuarto da cuenta de lo que viene más adelante, incluyendo la discusión sobre una propuesta de solución tecnológica, y, finalmente, el quinto capítulo hace un breve recuento y deja unas conclusiones.

II. Fundamentos de la responsabilidad de los intermediarios

II.A. La teoría del guardián o ama de llaves

La mayoría de nuestras actividades están mediadas por personas, instituciones y espacios privados que posibilitan y a la vez definen la manera en que las desarrollamos. El empleado de la aerolínea es el encargado de validar nuestros documentos para subirnos a un avión comercial, y solo a través de este servicio podemos viajar a otro país; la médica es quien nos entrega una autorización para adquirir un medicamento, y solo en ciertos lugares –farmacias y droguerías– podemos adquirirlo; el cajero del banco recibe un dinero que queremos girar al extranjero, y solo a través de este servicio –u otros semejantes– podemos hacer que llegue a su destino.

Esta interacción e interdependencia con actores privados es de especial interés para el Estado. En muchas ocasiones es más fácil para el regulador influir en la conducta del individuo a través de esos terceros que de manera directa. Así, le resulta más fácil al Estado que la aerolínea verifique si tenemos una visa vigente o que el banco cobre un impuesto por el dinero que enviamos al extranjero. Esta estrategia es conocida como teoría de intermediarios, amas de llaves o guardianes.

Según Emily Laidlaw, los guardianes o *gatekeepers* son agentes no estatales con la capacidad de alterar la conducta de terceros en circunstancias en que el Estado difícilmente puede hacerlo.[2] Usualmente al guardián le es indiferente la conducta que el Estado busca controlar, sin embargo, por los recursos, la información o la autoridad que posee, está en una posición ideal para regularla. Julia Black lo llama «regulación descentralizada», donde el núcleo de la actividad reguladora se mueve del Estado a espacios privados.[3]

---

[2] Cfr. Laidlaw, E., «A framework for identifying Internet information gatekeepers», *International Review of Law, Computers and Technology,* 24:3, p. 264.

[3] Cfr. Laidlaw, *supra* nota 2, p. 264.

Por mandato legal, los guardianes o amos de llaves controlan entonces el acceso a un servicio o insumo: la médica emite la fórmula para que el paciente no abuse del uso de un medicamento; la aerolínea bloquea el paso a inmigrantes ilegales a través de su servicio; el tendero sólo vende cigarrillos a mayores de edad. En todos los casos hay una actividad legalmente indeseable que el intermediario previene o controla. «Este respaldo, usualmente en la forma de un bien especializado o una forma de certificación esencial para que la irregularidad prospere, es la 'compuerta' que el guardián vigila», explica Reinier Kraakman.[4]

Algunos intermediarios son guardianes por la naturaleza misma del servicio o el insumo que prestan. Por ejemplo, la aerolínea es un paso obligado para quien quiere viajar en avión (a menos que usted sea Carlos Slim y tenga uno propio) y, hablando específicamente de Internet, la empresa que provee la conexión es un paso obligado para que podamos acceder a la red. Por el contrario, otros agentes se vuelven guardianes por creación legal. Es el caso del médico que se vuelve un guardián virtual y ejerce como punto de control entre el paciente y el acceso a los medicamentos.

El uso de intermediarios para regular ciertos comportamientos surge como alternativa frente a las limitaciones o riesgos de la intervención estatal directa sobre el ciudadano. Por un lado, al Estado le resulta imposible o demasiado dispendioso desincentivar o castigar cierta conducta –el abuso de una droga, la inmigración ilegal– enjuiciando a cada persona de manera individual. Por el otro, la imposición de penas altas para desestimular dicha conducta puede tener un efecto desproporcionado frente a personas que no están incurriendo en ella pero temen el castigo por cuenta de un error propio o de una aplicación equivocada de la ley.[5] En otras palabras, controlar el acceso a un medicamento o impedir la inmigración ilegal no puede desembocar en que la gente prefiera no adquirir un medicamento o dejar de viajar al extranjero.

Decíamos que al guardián generalmente no lo afecta la posible conducta irregular del individuo. Para la médica puede resultar indiferente que el paciente compre drogas no prescritas; para la aerolínea puede ser irrelevante que el pasajero no tenga una visa válida; al prestador del servicio de Internet no lo afecta que un usuario descargue música ilegal. Es bajo ese presupuesto,

---

[4] Cfr. Kraakman, R., «Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy», *Journal of Law, Economics and Organization*, II:1, Yale Law School, 1986, p. 54.

[5] Cfr. Kraakman, *supra* nota 4, p. 57.

entonces, que la estrategia de usar guardianes o amas de llaves debe incluir incentivos legales para que los intermediarios colaboren. Y la mejor manera es haciéndolos responsables legalmente por la conducta indeseada del tercero, a menos que asuman ciertas obligaciones. Este diseño regulatorio se traduce en mecanismos y obligaciones concretas que le permitan al guardián detectar la conducta o el riesgo, bien sea para prevenir que suceda del todo o para minimizar su ocurrencia.

Las obligaciones que asume el guardián dependen en gran medida de qué tipo de rol tiene. La teoría se refiere, en general, a dos tipos de guardianes: el «bouncer» y el «chaperón». El «bouncer» –siguiendo la figura del empleado que controla la entrada a la discoteca– simplemente se niega a proveer el servicio o autorizar el acceso; el «chaperón», por su parte, establece una relación con el tercero y lo acompaña y lo vigila para que no incurra en la acción indeseada.[6] Y mientras el bouncer tiene que tomar decisiones entre lo que es y no es aceptable –situaciones de sí o no, de blanco o negro–, el chaperón tiene una misión más compleja: al desarrollar una relación con el sujeto y al estar prestándole un servicio, debe monitorearlo y a la vez influir en su conducta.

Es fundamental considerar el balance entre los costos que asume el intermediario y los beneficios que obtiene por ejercer su rol de guardián –como «bouncer» o «chaperón»–. Un desequilibrio entre unos y otros implica una estrategia fallida de amo de llaves, lo cual impacta negativamente a terceros e inhibe actividades socialmente deseables. Kraakman distingue cuatro factores clave para instaurar un esquema de guardianes o amas de llaves:[7]

i) Existe una conducta indeseada que no se logra disuadir a través de las sanciones existentes. Éste es el punto de partida. Como ya se señaló, la idea del Estado de usar intermediarios pasa por el análisis previo de la conveniencia para el fin propuesto. Si existen mejores alternativas a través de las sanciones existentes y del poder directo del Estado, el uso de guardianes es una estrategia equivocada.

ii) No hay incentivos privados suficientes para que los guardianes intenten controlar o detener dicha conducta. Si al intermediario le conviene controlar la conducta, la mejor alternativa para el Estado puede ser abstenerse de intervenir en la relación entre aquel y el ciudadano. Por ejemplo, a un centro comercial le conviene que sus almacenes no vendan productos robados o que

---

[6] Cfr. Zittrain, Jonathan, «A History of Online Gatekeeping», *Harvard Journal of Law & Technology*, Vol. 19, N° 2, Spring 2006, ps. 253-298.

[7] Cfr. Kraakman, *supra* nota 4, p. 61.

las zonas comunes sean seguras para los visitantes. Instaurar un incentivo legal para obligar a que el centro comercial controle ambos frentes puede ser innecesario y, al contrario, puede generar costos que antes no existían.

iii) Existen intermediarios que pueden prevenir la conducta indeseada de manera confiable sin importar qué alternativas hay en el mercado para los infractores. El uso de guardianes tiene sentido si éstos pueden prevenir o controlar la conducta en una escala y medida razonable. Al contrario, no parece adecuada como política pública si, a pesar de algunas amas de llaves rigurosas, la conducta indeseada se lleva a cabo por otras vías –mediante intermediarios flexibles o mercados negros ampliamente disponibles–. De ser así, el efecto negativo es múltiple: el intermediario incurre en costos ineficientes, sólo los asume el ciudadano que no desea incurrir en la conducta indeseada, y ésta no se ve afectada (aún peor, los más interesados en perpetrarla serán los primeros en buscar alternativas). Como contra-argumento puede decirse que tener algunos intermediarios ejerciendo como guardianes sirve para mover la conducta a espacios marginales y, por lo tanto, para desalentar la conducta en el grueso de la población.

iv) Los costos para inducir a los intermediarios a que colaboren son razonables. Este último punto está relacionado con todos los anteriores. Si partimos del supuesto de que al intermediario le es indiferente que el ciudadano incurra en la actividad indeseada, los costos que éste debe asumir deben ser razonables para que colabore con el Estado. Por supuesto, el Estado puede ejercer su poder punitivo contra un intermediario –en el fondo el incentivo no es otra cosa que una amenaza de sanción legal–. Pero el problema radica en que ante costos muy altos el intermediario optará por no prestar el servicio (así como un futuro intermediario preferirá no aventurarse a ofrecerlo del todo), o lo hará en condiciones deficiente o demasiado gravosas para el beneficiario. En esos términos, la estrategia de ama de llaves podrá lograr el control de una actividad indeseada, pero acabará por afectar otras necesarias y, a la postre, tal vez más importantes.

La teoría sobre guardianes o amos de llaves también aparece, entre otros, en los estudios académicos sobre medios masivos de comunicación. En ese contexto, el rol central de los medios en la sociedad consiste en «escoger y moldear un sinnúmero de pedazos de información para volverlos un número limitado de mensajes que llegan a la gente diariamente».[8] En ese proceso, el

---

[8] Shoemaker, P., *Gatekeeping Theory,* Routledge, 2009, Introducción. Traducción informal.

medio es el intermediario principal –el guardián de lo que entra o queda fuera del debate público–.

Basándose tanto en esta aproximación como en la general, Barzilai-Nahon considera que la teoría sobre guardianes tiene unas características propias en Internet. En un contexto interconectado, con nodos y relaciones dispares, el principal rol del guardián –paralelo al ejercicio de su servicio– es controlar el flujo de información. Este rol abarca tres objetivos: amurallar al usuario (o «encerrado») en la red del guardián, ejercer la guardia para evitar que agentes externos al entorno cerrado atraviesen el portón, y mantener sin sobresaltos la actividad permitida dentro de la red.[9]

II.B. La responsabilidad civil

La doctrina sobre responsabilidad civil extracontractual –similar al *tort* en países de *common law*– también ha sido propuesta para resolver el vacío sobre la responsabilidad de los intermediarios de Internet frente a los hechos cometidos por sus usuarios. En la medida en que se trata de un riesgo legal que genera un incentivo para controlar una actividad indeseada, tiene alguna relación con la teoría del guardián. El planteamiento básico es el siguiente: un intermediario puede llegar a ser responsable bien sea por los daños que cause un usuario o porque gracias al servicio que aquel presta fue que se produjo y potenció el daño.

Tomemos un ejemplo: a través de Twitter una persona difunde rumores falsos sobre otra, por cuenta de los cuales ésta última pierde su trabajo y la posibilidad inminente que tenía de hacer un negocio. Bajo un análisis general de responsabilidad civil, la persona afectada podría iniciar una acción judicial contra Twitter para buscar que se le repare el daño. En ese caso, tendría que probar ante el juez que efectivamente el daño existió, que hay un nexo causal entre ese daño y la actuación de Twitter, y que Twitter fue negligente a la hora de evitarlo.

Más allá de que bajo este análisis el intermediario puede terminar respondiendo por la actuación de sus usuarios, éste sería el enfoque menos gravoso para Twitter, ya que implica demostrar que estuvo involucrado directamente

---

[9] Barzalai-Nahon, K., «Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control», *Journal of the American Society for Information, Science and Technology,* 59(9), 2009, ps. 1493-1512.

en el hecho indeseado. Sin embargo, dentro del mismo régimen de responsabilidad civil se han propuesto alternativas que pueden hacer más exigente el deber del intermediario: la responsabilidad por el hecho de otro y la actividad peligrosa.

Por regla general, una persona debe responder legalmente por los daños que cause. Dependiendo de la gravedad de la conducta, la persona puede estar obligada a resarcir económicamente al afectado e, incluso, puede estar sujeta a una sanción penal. Es lo que acabamos de ilustrar. No obstante, una persona también puede ser responsable por los hechos de otra persona o un objeto a su cargo. Es el caso, por ejemplo, del daño causado por un hijo o una mascota, y se conoce como responsabilidad por el hecho de otro.[10]

En este renglón de la responsabilidad civil, y siguiendo con el ejemplo, se parte del supuesto de que los daños que puedan producir los usuarios de Twitter a través de la plataforma son responsabilidad de Twitter. Y aunque la carga probatoria para el afectado es similar al del escenario anterior, el intermediario tendría un deber de vigilancia más complejo, lo que implica demostrar que obró con diligencia para supervisar las acciones del usuario (haber actuado como un «buen padre de familia»).

Por último, está la responsabilidad objetiva, y específicamente la tesis de que la actividad de un intermediario como Twitter implica la creación de un riesgo público –tanto como la extracción de minerales con explosivos o el uso de armas por parte del Estado–. Bajo este estándar, y volviendo al ejemplo, habría una presunción de que la actividad que desarrolla Twitter es peligrosa y, por lo tanto, tendría que ser éste el que pruebe que el daño se produjo por un hecho imposible de prever o por fuera de su órbita de control.

La idea de instaurar un régimen de responsabilidad objetiva para los intermediarios de Internet fue impulsada principalmente por las industrias creativas para proteger el derecho de autor.[11] Pero esta propuesta no tiene mayor vigencia hoy en día. Ante un riesgo de responsabilidad objetiva –y de una san-

---

[10] Cfr. Mazeaud, H. y Mazeaud, L., *Compendio del tratado teórico y práctico de la responsabilidad delictuosa y contractual,* t. I, Colmez, México, 1945.

[11] Cfr. Jessica Litman en *Digital Copyright. Selected Works*, 2006; Peguera Poch, M., «La exención de responsabilidad civil por contenidos ajenos en Internet», Jornadas de Responsabilidad Civil y Penal de los Prestadores de Servicios en Internet, Barcelona, noviembre de 2001, disponible en: http://www.uoc.edu/in3/dt/20080/#bibliografia (consultada el 6 de agosto de 2013).

ción pecuniaria cuantiosa– el intermediario podría optar por no prestar el servicio o implementaría cambios estructurales para ofrecerlo en condiciones sumamente controladas. Refiriéndonos por última vez al ejemplo, llevaría a Twitter a instaurar un sistema para verificar los contenidos antes de su publicación, o a no ofrecer el servicio del todo. Y en términos de la estrategia de crear un guardián o ama de llaves, generaría efectos no deseados o amenazaría la existencia misma del intermediario.[12]

Los demás planteamientos sobre la responsabilidad extracontractual –por el daño producido y por el hecho del tercero–, aún tienen vigencia. Por un lado, apuntalan algunas de las leyes existentes y, por el otro, algunos jueces los han aplicado en procesos judiciales contra intermediarios. En este caso, un elemento problemático ha sido determinar en qué consiste, concretamente, la diligencia a la que está obligado el intermediario para eximirse de responsabilidad (esto es, por ejemplo, si debe bloquear contenidos, monitorear permanentemente el servicio o atender la queja de una persona afectada, entre otros). Se trata, en última instancia, de otra manera de llegar a la pregunta de en qué consiste la guardia que debe llevar a cabo el guardián. A esto volveremos más adelante.

III. Los antecedentes: metiendo a las ovejas al redil

III.A. Los intermediarios como editores o distribuidores

Zittrain ubica el origen de los primeros debates judiciales sobre responsabilidad de intermediarios de Internet en Estados Unidos en decisiones de los noventa. Para entonces, aunque el *World Wide Web* era apenas una idea en marcha y no había las aplicaciones que hoy conocemos, varias empresas suministraban simultáneamente la conexión y una navegación limitada a los confines de sus servicios.[13] En ese entonces los usuarios compartían información y publicaban mensajes en el tablero (*bulletin board*) del operador, un espacio sin configuraciones sofisticadas ni fines específicos.

---

[12] Cfr. Hylton, K., *Property Rules, Liability Rules, and Immunity: An Application To Cyberspace,* Boston University School of Law, Working Paper Series, Law and Economics Nº 06-19, 2006. Ver, también, Carrasco Blanc, H., «Algunos aspectos de la responsabilidad de Proveedores de Servicios y Contenidos de Internet. El caso ENTEL», *REDI*, Nº 26, agosto de 2000.

[13] Cfr. Zittrain, *supra* nota 6.

Que la principal actividad en Internet en ese entonces fuera la difusión de contenidos llevó a que se buscaran analogías entre los intermediarios de este espacio naciente y los medios de comunicación tradicionales. «Los primeros debates jurisprudenciales y legislativos sobre cómo categorizar el Internet giraron en torno a si clasificar a los intermediarios usando los modelos tradicionales de medios escritos, radiodifundidos y de transmisión común», afirma Laidlaw.[14] El punto central era definir alguna responsabilidad similar para esos actores por la difusión de contenidos difamatorios que hacían sus usuarios.

Optar por una u otra categoría implicaba asignarles niveles distintos de responsabilidad por lo que se dijera o transmitiera. Si el intermediario era considerado como un medio escrito, podría responder por cualquier contenido que pasara por o estuviera en su servicio. En cambio, si era considerado un transmisor común o *common carrier* –como cualquier compañía de teléfonos o de servicio postal– no tendría que responder por lo que dijeran o hicieran sus usuarios.

Los casos a los que se refiere Zittrain son los siguientes: en 1990, la empresa Cubby Inc. demandó por difamación a Compuserve por cuenta de un material producido por un particular pero distribuido por este operador a sus suscriptores. De manera similar, en 1994 una firma inversionista demandó a Prodigy por una acusación de fraude hecha por un usuario anónimo –esta vez a través de un foro sobre temas económicos–.[15]

Ante la ausencia de legislación específica (la cual llegó poco después), los jueces acudieron al precedente análogo. Según éste, aunque tanto una editorial como un medio de comunicación pueden llegar a ser responsables legalmente, el estándar es más bajo para el primero. De manera general se considera que la editorial es un mero distribuidor o conductor pasivo de un contenido –los libros–, mientras el medio de comunicación interviene en lo que se publica –el periódico o la revista– y, por lo tanto, tiene injerencia en éste. Esta distinción fue la base para que los jueces resolvieran los casos por vías distintas: Compuserve fue considerado como un simple distribuidor de la informa-

---

14 Laidlaw, *supra* nota 2, p. 265. Traducción informal.

15 Cfr. *Cubby vs. Compuserve*, en Digital Media Law Project, disponible en: http://www.dmlp.org/threats/cubby-v-compuserve, y *Stratton Oakmont vs. Prodigy*, en Digital Media Law Project, disponible en: http://www.dmlp.org/threats/stratton-oakmont-v-prodigy (consultadas el 2 de agosto de 2013).

ción de terceros –una especie de *common carrier*– y Prodigy, como un editor. Es decir: el primero fue declarado inocente y el segundo, culpable.

La idea de que los prestadores de servicios de Internet (PSI) respondieran por la actividad de sus usuarios no se limitaba al problema de la difamación en línea. Ya para finales del siglo XX parecía claro que el entorno digital, más allá de la promesa de acceso al conocimiento, desarrollo y libertad de expresión, abría un espacio para la distribución de pornografía infantil, la comisión de delitos como la estafa o el robo de identidad y, por supuesto, el tráfico no autorizado de películas y música.[16]

Este último tema era especialmente sensible en Estados Unidos. Los estudios discográficos y la industria cinematográfica –los principales titulares de contenido– veían Internet como una amenaza para su negocio, y presionaron al gobierno para que expidiera legislación que hiciera responsables a los PSI por los contenidos ajenos que compartían sus usuarios. Sin entrar en disquisiciones teóricas sobre qué responsabilidad debían tener estos amos de llaves, le hicieron un ultimátum al gobierno de Bill Clinton (1993-2001), que en parte reflejaba la visión que tenían sobre Internet: si dicha protección no existía, no verterían sus contenidos en este nuevo espacio. Sería una red de tubos sin nada adentro. El resultado fue el *Digital Millennium Copyright Act* de 1998, una ley menos radical de lo que las industrias pretendían, pero con un régimen de responsabilidad concreto para los PSI.[17]

III.B. El fin de la excusa tecnológica

Según Lilian Edwards, los PSI –conscientes de que a través de sus redes y servicios se transmitía y alojaba contenido altamente riesgoso– venían planteando a su favor una razón práctica: «Los PSI argumentaron vigorosamente que no podían revisar manualmente la legalidad de todo el material que pasara por sus servidores sin incurrir en demoras y costos inconcebibles».[18] De

---

[16] Cfr. Edwards, L., «The Fall and Rise of Intermediary Liability Online», en *Law and the Internet*, Hart Publishing, Oxford y Portland, Oregon, 2009, ps. 47-88.

[17] Cfr. Cortés Castillo, C., «Mirar hacia el norte es mirar hacia atrás: el impacto negativo de la DMCA. El mecanismo de notificación y retiro y las Medidas Tecnológicas de Protección», *Documentos Karisma,* julio de 2013, disponible en: http://karisma.org.co/?p=2241 (consultada el 5 de agosto de 2013).

[18] Edwards, *supra* nota 16, p. 59. Traducción informal.

este argumento se desprendía otro igualmente importante, que era el riesgo de estancar el desarrollo, la innovación y la competencia en Internet (una razón estratégica para Europa, ya rezagada en el tema frente a Estados Unidos).

Esta postura, que sin duda fue determinante para la expedición de normas y decisiones judiciales favorables a los PSI, tuvo un punto de quiebre en 2000. Ese año un francés llamado Mark Knobel demandó a Yahoo en Francia por ofrecer en su portal objetos y recordatorios alusivos a los nazis (distribuir productos nazi es ilegal en ese país). «La justicia francesa quiere imponer su parecer en una área sobre la que no tiene control», comentó entonces el fundador de Yahoo Jerry Yang.[19] La respuesta fue contundente: «Existe esta idea naif de que Internet lo cambia todo. Pues no cambia todo. No cambia las leyes en Francia», dijo uno de los abogados del caso.[20] Para los demandantes, Yahoo bien podía vender todos los productos nazi que quisiera en Estados Unidos, pero no dentro de las fronteras de su país.

Yahoo se defendió, como era previsible, con el argumento de la «imposibilidad». Dijo que no tenía el poder para identificar de dónde venían sus compradores ni la manera de controlar quiénes accedían a sus productos digitales. Y si la empresa removiera la oferta de productos nazi de sus servidores en Estados Unidos, estaría dándole a la ley francesa un alcance mundial. Al juez no pareció impresionarle mucho el planteamiento, y le encargó a un comité que determinara si era posible filtrar automáticamente las solicitudes de contenido desde una localización en particular. La respuesta fue afirmativa, y sustentó la orden judicial. De la misma manera como Yahoo ya situaba publicidad diferenciada para usuarios de diferentes países, podía bloquear el acceso de la mayoría de los franceses a un contenido en particular –a partir de las direcciones IP y los datos de los usuarios–.[21]

Este caso suele usarse para ilustrar el problema de la jurisdicción –o, más bien, de la dispersión de jurisdicciones– en Internet.[22] Pero también es un ante-

---

[19] Carr, N. *The Big Switch: Rewiring the World, From Edison to Google,* W. W. Norton & Company, 2013, p. 199. Traducción informal.

[20] Goldsmith, J.; Wu, T., *Who Controls the Internet? Illusions of a Borderless World,* Oxford University Press, 2006, p. 2. Traducción informal.

[21] Cfr. Edwards, *supra* nota 16. Traducción informal.

[22] Sobre este tema, ver Bertoni, E., «La determinación de la jurisdicción en litigios por difamación por contenidos en Internet: algunas observaciones para América Latina», en Bertoni, E. (comp.), *Hacia una Internet libre de censura. Propuestas para América Latina,* Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Facultad de Derecho, Universidad de Palermo, 2012, ps. 313-339.

cedente fundamental para comprender cómo se fue construyendo –para bien o para mal– el rol de los PSI como guardianes. Una vez desmontado el argumento de la imposibilidad (que aunque pudo ser cierto en un momento no era inmutable), se abrió paso la discusión sobre qué tipo de obligaciones debían tener los PSI como amos de llaves de los usuarios. Y a partir de allí la tecnología dejaba de ser un obstáculo para convertirse en el instrumento que les permitiría a los PSI, tanto por obligación como por conveniencia, ejercer ese papel.

IV. Los guardianes y su deberes: tipos de intermediarios y responsabilidades

Los intermediarios en línea son, entonces, todos los agentes que de una u otra manera posibilitan y determinan nuestra actividad en Internet. No todos están ubicados en el mismo nivel en la red ni ofrecen el mismo servicio. En una arquitectura de niveles como la de Internet, unos están en la capa física –son la infraestructura de la red– y otros en la de aplicaciones.[23] Y en ésta última son diversos los servicios y las formas de usabilidad para el usuario.

Estas diferencias se concretan en las clasificaciones sobre los tipos de intermediarios. En general, se habla de los que posibilitan el acceso a la red (la empresa a la que pagamos por el servicio de Internet), por un lado, y todos los demás que ofrecen servicios en línea, por el otro (Google, Facebook, Dropbox, Amazon, nytimes.com, etc.). Pero hay clasificaciones más detalladas y variadas.

Mann y Belzley se refieren a los Prestadores de Servicios de Internet (PSI), que proveen la conexión y alojan los contenidos; los intermediarios de pago, que posibilitan transacciones económicas (como Paypal o Visa) y los intermediarios de subasta, que ofrecen a la venta productos de terceros (como Ebay o Mercadolibre).[24] De manera similar, Meléndez Juarbe plantea la división entre intermediarios de conexión, de información y financieros.[25] Y Zunino

---

23 Sobre la arquitectura de la red, ver Cortes Castillo, C., *Vigilancia de la red: ¿qué significa monitorear y detectar contenidos en Internet?,* en esta misma obra.

24 Cfr. Mann, R. y Belzley, S., «The Promise of Internet Intermediary Liability», *Law and Economics Working Paper,* N° 45, abril de 2005, The University of Texas School of Law, ps. 1-51.

25 Meléndez Juarbe, H., «Intermediarios y libertad de expresión: apuntes para una conversación», en Bertoni, E. (comp.), *Hacia una Internet libre de censura. Propuestas para América Latina,* Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Facultad de Derecho, Universidad de Palermo, 2012, ps. 109-123.

los divide en operadores de redes y proveedores de acceso, proveedores de servicios de búsqueda y enlaces (por ejemplo, Google), y prestadores de servicios de almacenamiento de datos (como Dropbox o Box.net).[26]

Estas clasificaciones suelen actualizarse para tratar de reflejar de manera más precisa el panorama de intermediarios en la red. Y aunque el ejercicio puede quedarse corto frente a la evolución y convergencia de algunos servicios (piénsese, por ejemplo, que hoy por hoy Google ofrece tanto servicios de almacenamiento como de búsqueda), el punto central es entender que estas categorizaciones se hacen con la idea de identificar al intermediario para saber qué función debe asumir como guardián.

En materia de flujo de contenidos en Internet,[27] la mayoría de leyes sobre responsabilidad de intermediarios se han expedido para que el guardián ayude a enfrentar uno de tres problemas: la pornografía infantil, la piratería o las vulneraciones al honor y el buen nombre. En ninguno de estos casos se ha establecido un régimen de responsabilidad objetiva. Las leyes varían entre lo que se conoce como una inmunidad total o una inmunidad condicionada para el intermediario. Y en países sin leyes específicas, los jueces han resuelto algunos casos en estos mismos temas a partir del régimen general de responsabilidad civil (en América Latina, especialmente en Argentina). A continuación se abordan los tres ámbitos, tomando un ejemplo y haciendo énfasis en los deberes que implica para el intermediario.[28] Igualmente, se señalan algunas críticas comunes frente a estos modelos.

IV.A. Inmunidad absoluta

Para explicar el régimen de inmunidad absoluta vamos a tomar el caso de Estados Unidos. En 1996, el Congreso de ese país expidió el *Communications*

---

[26] Cfr. Zunino, M., «La responsabilidad de los proveedores de servicios de Internet y la libertad de expresión», *La Ley*, 31 de octubre de 2012.

[27] Como se mencionó en la introducción, este documento se centra en la responsabilidad de intermediarios frente a contenidos. No se abordan temas relacionados con comercio electrónico o delitos como estafa en línea.

[28] Para un estudio comparado sobre las normas en la materia, ver, Ruiz, C. y Lara, J., «Responsabilidad de los proveedores de servicios de Internet en relación con el ejercicio del derecho a la libertad de expresión en Latinoamérica», en Bertoni, E. (comp.), *Hacia una Internet libre de censura. Propuestas para América Latina,* Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Facultad de Derecho, Universidad de Palermo, 2012, ps. 109-123.

Decency Act (CDA) con el propósito principal de combatir la pornografía y la obscenidad en línea. Por encontrarla contraria a la Primera Enmienda –que protege la libertad de expresión–, un año después la Corte Suprema de Justicia tumbó la mayor parte de la norma. Sin embargo, dejó vigente la Sección 230, que establece que ningún proveedor o usuario de un «servicio informático interactivo» puede ser tratado como editor o portavoz de la información proporcionada o difundida por cualquier otro usuario o servicio.[29]

En otras palabras, los intermediarios que alojan, publican o «repostean» información o expresiones de terceros están protegidos de eventuales acciones judiciales por difamación o similares. Ningún titular de un servicio como Twitter o Facebook, ningún medio de comunicación en línea y ninguna persona con un blog o página personal, es responsable por los comentarios o los contenidos –ya sea texto, audio o video– que otras personas difundan a través del servicio o en el portal respectivo.

Esta inmunidad absoluta no era la intención del legislador. El texto original de la ley incluía unas provisiones «antiobscenidad», según las cuales podía ser criminalmente responsable quien, entre otras, usara un «servicio informático interactivo» para poner a disposición de un menor de 18 años cualquier comentario, sugerencia, propuesta, imagen o contenido que, de conformidad con los estándares contemporáneos de una comunidad, describiera o representara actividades sexuales o escatológicas. En su revisión de esta disposición, la Corte Suprema subrayó la relevancia de la libertad de expresión y la necesidad de que las normas que se relacionen con este derecho no sean desproporcionadas:

> «La CDA carece de la precisión que la Primera Enmienda requiere cuando un estatuto regula el contenido de la expresión. Si bien el gobierno tiene un interés en proteger a los niños de material potencialmente dañino, la CDA persigue ese interés suprimiendo una gran cantidad de expresión que los adultos tienen derecho constitucional de enviar y recibir. Su alcance no tiene precedentes. La carga que la CDA impone en la expresión de los adultos es inaceptable si alternativas menos restrictivas podrían ser al menos igual de efectivas para alcanzar los objetivos legítimos de la ley».[30]

---

[29] Ver 47 USC § 230 - Protection for private blocking and screening of offensive material, disponible en: http://www.law.cornell.edu/uscode/text/47/230 (consultada el 6 de agosto de 2013).

[30] Corte Suprema de los Estados Unidos, *Reno v. American Civil Liberties Union,* 521 U.S. 844, junio 26 de 1997, disponible en: http://www.law.cornell.edu/supct/html/historics/USSC_CR_0521_0844_ZS.html. Traducción informal.

El razonamiento de la Corte también puede leerse en clave de guardianes y amas de llaves. En su versión original, la CDA introducía el incentivo de la sanción para que los intermediarios colaboraran con la conducta indeseada. Pero los costos de este esquema no eran razonables, no solo para los prestadores del servicio –que habrían tenido que introducir sistemas de monitoreo y vigilancia–, sino también, y principalmente, para el grueso de la sociedad. El costo que se pagaba, la externalidad negativa, era la restricción abierta e inconmensurable del debate público.

Los defensores de la libertad de expresión consideran que la inmunidad absoluta de la CDA es una conquista, y prenden las alarmas cuando se escuchan propuestas de pasar normas similares a la versión original.[31] No sin razón, consideran que una norma distinta posibilitaría el control de contenidos con fines políticos, la censura previa y, en general, una inhibición de la libertad de expresión en línea. No obstante, poco a poco surgen voces autorizadas para quienes la balanza está excesivamente desequilibrada en contra de derechos como la privacidad o el buen nombre.

«La velocidad con la que las reputaciones pueden construirse y alterarse es solo una de las formas en que Internet ha cambiado todo. Con seguridad, la mayoría de estos cambios han sido para bien, pero lamentablemente Internet es una maldición cuando el objeto de información negativa es uno», afirman Levmore y Nussbaum.[32] Para éstos y otros autores, es poco o nada lo que pueden hacer los usuarios afectados frente a la propagación de rumores, el abuso del anonimato, el lenguaje obsceno y abusivo, y la misoginia.

Solove y Leiter, entre otros, proponen que la Sección 230 del CDA se modifique para abandonar un régimen de inmunidad total. «El daño de la expresión en Internet es suficientemente serio para que debamos repensar las protección legales», afirma Leiter.[33] Por su parte, Solove critica el hecho de

---

[31] Ver, por ejemplo, «Section 230 Under Attack: State AGs' Proposal Threatens Internet As We Know It», Center for Democracy and Technology, julio de 2013, disponible en: https://www.cdt.org/blogs/andrew-mcdiarmid/2507section-230-under-attack-state-ags%E2%80%99-proposal-threatens-internet-we-know-i (consultada el 6 de agosto de 2013).

[32] Levmore, S. y Nussbaum, M. (eds.), *The Offensive Internet. Speech, Privacy, and Reputation,* Harvard University Press, Cambridge, 2010, pos. 45 (versión Kindle). Traducción informal. Ver, también, Lemley, M., «Rationalizing Internet Safe Harbors», *Journal of Telecommunications and High Technology Law*, Vol. 6, 2007, p. 101.

[33] *Ibídem*, pos. 1960.

que la mayoría de la cortes hayan extendido la inmunidad para los intermediarios incluso cuando tienen conocimiento de que el material es difamatorio. En consecuencia, propone que se instaure un sistema de notificación y retiro o notificación y respuesta, un sistema que –como veremos– entraña a su vez otros problemas.[34]

IV.B. Inmunidad condicionada

La inmunidad condicionada la encontramos sobre todo en normas sobre protección de derechos de autor en Internet. La idea de este tipo de regímenes es ofrecerle al intermediario un «puerto seguro» donde esté a salvo de cualquier responsabilidad legal siempre y cuando cumpla con deberes concretos. Aunque los titulares de contenido abogaron por un nivel de responsabilidad mayor, la inmunidad condicionada terminó siendo el punto de encuentro entre los intereses de éstos y de los Prestadores de Servicios de Internet (PSI).[35]

La sección 512 del *Digital Millenium Copyright Act* (DMCA) de Estados Unidos, expedido en 1998, estipula unas condiciones para que un PSI no sea responsable por las posibles violaciones a los derechos de autor llevadas a cabo por sus usuarios. Si el PSI cumple con esas condiciones entra en el puerto seguro de la ley, en cuyo caso el titular del contenido no podrá perseguirlo legalmente por un eventual daño.

El DMCA establece unas categorías de PSI que están amparados por la ley.[36] El propósito es asegurarse de que éstos actúan realmente como intermediarios y no como distribuidores directos del contenido protegido. A partir de esta clasificación, la ley parte del supuesto de que los PSI no tienen por qué saber si un usuario está usando de manera ilegal el contenido de terceros. Es decir, el DMCA no establece un deber permanente de monitoreo. Sin embargo, esta presunción se desvirtúa cuando algún hecho o circunstancia indica

---

34 *Ibídem*, pos. 806.

35 Ver, entre otros, Drahos, P. y Braithwate, J., *Information Feudalism. Who Owns the Knowledge Economy*, The New Press, Nueva York y Londres, 2002; Decherney, P., *Hollywood's Copyright Wars. From Edison to the Internet,* Columbia University Press, Nueva York, 2012; Jessica Litman en *Digital Copyright. Selected Works,* 2006.

36 La DMCA admite cuatro categorías de intermediarios: los que conducen, transmiten o enrutan información, los que hacen copias temporales (*caching*), los que almacenan información y los que ayudan a localizar información –referido principalmente a los motores de búsqueda–.

que hay una actividad infractora manifiesta o cuando el titular del material notifica al PSI.

Desde ese momento el PSI ya tiene conocimiento de una posible infracción al derecho de autor y, por lo tanto, empieza a abandonar el puerto seguro. Conoce de una posible actividad infractora y la está permitiendo. En consecuencia, si el PSI quiere mantener su inmunidad, debe proceder a bloquear el acceso al material o retirarlo –un video, por ejemplo– y notificar al usuario afectado de lo sucedido.[37] Y si el usuario afectado considera que el material fue removido o bloqueado erróneamente, puede iniciar un proceso de contra-notificación. No obstante, debe estar dispuesto a llevar su caso ante cualquier juez y esperar un lapso de entre 10 y 14 días.[38] Pasado ese término, si el titular del contenido no inició una acción judicial, el PSI debe restablecer el contenido.

Como estrategia de ama de llaves, la inmunidad condicionada del DMCA establece un incentivo claro para el guardián, y aunque impone costos considerables –el PSI debe tener un responsable en su empresa para atender estos procedimientos– no impone deberes difusos o desproporcionados de monitoreo y vigilancia.[39] Los costos, en cambio, sí los asumen los usuarios y la comunidad en general.

De una parte, el usuario que resulta afectado por un retiro equivocado corre con el costo de «perder» el contenido –al menos temporalmente– y asume la carga de defenderlo. De otra parte, la comunidad en general resulta

---

[37] Esta obligación no está en cabeza de los intermediarios que enrutan o transmiten información y de aquellos que hacen copias temporales. Si no originan la transmisión ni manipulan los datos más allá de lo que técnicamente se requiera, están en una especie de inmunidad absoluta (como si fueran *common carriers*).

[38] Para una explicación más detallada sobre la DMCA y el «puerto seguro», ver Cortés Castillo, *supra* nota 17.

[39] De manera similar a la DMCA, la Directiva sobre el comercio electrónico de la Unión Europea establece que los prestadores de servicios no tienen una obligación general de supervisión. Esto significa, concretamente, que los Estados parte no les impondrán a éstos «una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas»; Directiva 2000/31/CE, Diario Oficial, N° L 178 de 17/7/2000, p. 0001 - 0016, disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:ES:HTML (consultada el 5 de agosto de 2013).

afectada por las expresiones e informaciones removidas de manera excesiva. Por cuenta del balance de los incentivos, el PSI no pierde nada con retirar material y sí gana mucho con la entrada al puerto seguro.[40]

Según Lemley, «el efecto del sistema de notificación y retiro ha sido fomentar que los intermediarios de Internet bajen cualquier contenido que protesten los titulares de derecho de autor, sin importar cuán frívola pueda ser la queja».[41] En la misma línea, para Tushnet, «el proceso de notificación y retiro puede usarse para suprimir tanto discursos críticos como infracciones al derecho de autor».[42]

En contraste con el mecanismo de notificación y retiro del DMCA, diversos países han optado por alternativas que mantengan los incentivos para los intermediarios pero, a la vez, brinden las garantías necesarias a los usuarios. La ley chilena sobre este tema –que implementa una de las obligaciones del tratado de libre comercio con Estados Unidos– incluye un mecanismo de retiro de contenido con intervención previa del juez.[43] Por otra parte, la ley canadiense incorpora un mecanismo de «notificación y notificación»: el reclamo del titular del contenido no obliga al PSI a retirar el contenido sino a notificar al usuario, y solo si el PSI incumple con este deber puede incurrir en una responsabilidad legal.[44]

Explicar en mayor detalle las distintas alternativas de puertos seguros y los debates que las rodean requeriría de un espacio aparte. Para efectos de este documento, es relevante tener en cuenta el balance entre los incentivos y los

---

[40] Cfr. Seltzer, W., «Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment», *Harvard Journal of Law and Technology*, Vol. 24, Nº 1, Fall 2010, ps. 171 y ss.

[41] Lemley, *supra* nota 32, p. 114. Traducción informal.

[42] Tushnet, R., «Power Without Responsibility: Intermediaries and the First Amendment», *The George Washington Law Review*, Vol. 76, Nº 4, 2008, p. 118. Traducción informal.

[43] Cfr. Álvarez Valenzuela, D., «En Busca de Equilibrios Regulatorios: Chile y las Recientes Reformas al Derecho de Autor», ICTSD, Documento de Política Pública, 22, 2011, disponibe en: http://ictsd.org/downloads/2011/12/en-busca-de-equilibrios-regulatorios-chile-y-las-recientes-reformas-al-derecho-de-autor.pdf (consultada el 6 de agosto de 2013).

[44] Cfr. Copyright Modernization Act, sección 41.25 y ss., disponible en: http://laws-lois.justice.gc.ca/eng/annualstatutes/2012_20/FullText.html# (consultada el 6 de agosto de 2013).

costos de la inmunidad condicionada, no solo para el intermediario sino también para el usuario y la comunidad en general. Igualmente, es fundamental observar que en la mayoría de estos sistemas de inmunidad condicionada el intermediario está exonerado de un deber permanente de monitoreo, lo cual resulta beneficioso. La inmunidad condicionada –siguiendo la tipología propuesta por Kraakman– vuelve a los PSI chaperones del usuario, pero de manera limitada. Esto se traduce en mayor libertad y autonomía para el ciudadano.

IV.C. Responsabilidad subjetiva

Por último tenemos los regímenes de responsabilidad subjetiva que –como vimos– no corresponden a la aplicación de una ley específica sobre intermediarios en Internet, sino al uso de normas y principios generales sobre responsabilidad civil. Decíamos atrás que éste puede ser un régimen menos gravoso para el intermediario en comparación con el de responsabilidad objetiva; no obstante, resulta más desventajoso frente a una inmunidad condicionada –ni qué decir de una absoluta– toda vez que los deberes del PSI no están del todo definidos. Para hablar de esta categoría vamos a centrarnos en un caso argentino (país en el que no hay ley de intermediarios en Internet).

En 2008 Esteban Bluvol se enteró de que existía un blog en Blogger (plataforma de Google) con su nombre y con material injuriante sobre él. Demandó a Google por daños y perjuicios a su vida personal y laboral, y en primera instancia el juez decretó a su favor una indemnización de diez mil pesos argentinos (unos US$1,800). Bluvol apeló el fallo para exigir una indemnización mayor y, en diciembre de 2012, la Cámara Nacional de Apelaciones de la Capital Federal aumentó la cuantía al doble.[45]

Para el tema que nos ocupa, lo interesante del caso fueron los regímenes que aplicaron los jueces de ambas instancias. El de primera instancia consideró que la responsabilidad de Google era objetiva, específicamente por la teoría del riesgo creado (similar a la de la actividad peligrosa). El juez de segunda instancia desestimó esa tesis rápidamente. Consideró que un intermediario como Google no debe «responder en forma automática por las conductas ilícitas de terceros, teniendo en cuenta que en internet circulan millones de noti-

---

[45] Cfr. Poder Judicial de la Nación, Cámara Nacional de Apelaciones de la Capital Federal, «Bluvol, Esteban Carlos c/Google Inc. y otros s/daños y perjuicios» (Exp. n° 59.532/2009), Rec. N° 607.911, Juzg. N° 105.

cias, lo que torna extremadamente dificultoso el control previo de todo lo que se difunde. Ello implicaría obligar a las empresas a monitorear constantemente los miles de perfiles o comentarios que se suben cada minuto».[46]

Sin embargo, el juez no exoneró a Google ya que consideró que de todas formas había incumplido con su responsabilidad. Previo al proceso judicial, Bluvol se había quejado directamente ante la empresa por la existencia y los contenidos del blog (usando los mecanismos usuales de queja o denuncia de contenido) sin que aquella lo removiera. Google argumentó que no podía hacerlo sin una orden judicial. En contraste, para el juez el incumplimiento se configuró cuando Google se negó a retirar el blog después de la solicitud del afectado. En ese momento había tenido efectivo conocimiento del hecho dañoso y no había obrado con diligencia. Agregó, por último, que más que un caso de libertad de expresión se trataba de uno de suplantación.

El caso Bluvol no es el único en Argentina con un argumento similar frente a la responsabilidad del intermediario como guardián del usuario. En el caso de Belén Rodríguez contra Yahoo y Google, en el que la primera solicitaba que se eliminara de los motores de búsqueda cualquier referencia a páginas de contenido sexual asociadas a su nombre, el juez de segunda instancia afirmó:

> «No creo que este deber del explotador del motor de búsqueda de bloquear los contenidos ilícitos requiera una previa orden judicial, como lo sostiene cierta doctrina. Ese requisito no surge, en nuestro país, de norma alguna, y no resulta compatible con el deber de diligencia que recae sobre las demandadas (…). Por el contrario, basta a mi criterio con que hayan tomado conocimiento –en principio, mediante la comunicación del usuario- de la existencia del contenido nocivo para que se encuentren obligados a bloquearlo con prontitud, pues esa es la conducta esperable de un empresario diligente de la clase de las aquí demandadas».[47]

De estos casos se extraen al menos dos conclusiones: primero, no existe un deber de monitoreo y vigilancia general. Esto es positivo. Un deber difuso o abstracto de monitoreo implica en la práctica un estándar muy riguroso de responsabilidad, pues el guardián debe ejercer un rol complejo y permanente de

---

46 *Ibídem*.

47 Poder Judicial de la Nación, Sala Civil A, «Rodríguez, María Belén c/Google Inc. y otro s/Daños y Perjuicios», Juzgado Civil N° 95 (Exp. n° 99.613/2006).

chaperón. Tendría que vigilar todas las acciones del usuario. A la postre, con una guardia de este tipo «el guardián puede ser penalizado por un rango de malas conductas muchos más amplio del que en realidad puede detectar».[48]

Segundo, el deber de diligencia del PSI está atado a hacer juicios de valor sobre la legalidad de las acciones del usuario. Y esta facultad informal de adjudicación sí es problemática. ¿Cuál sería el criterio para que el intermediario mantenga o elimine un contenido cuando se trate de imputaciones fácticas o afirmaciones subjetivas? ¿Qué hace cuando se encuentra con versiones encontradas o zonas grises?

V. Mirando al horizonte: el riesgo del filtrado y la idea de la solución tecnológica

Los regímenes de responsabilidad para los intermediarios en Internet son, a la vez, la causa y la consecuencia de un proceso de estrechamiento del entorno digital. No es posible analizarlo aquí en detalle. Baste con decir que en él confluyen intereses del Estado –combatir el terrorismo, vigilar a los ciudadanos y proteger algunos derechos individuales, entre otros– y de los particulares –comercializar, sofisticar y controlar la experiencia en línea, principalmente–.[49] No se trata, sin embargo, de una evolución inevitable o lógica. Las alternativas y las divergencias frente a estos modelos también hacen parte de ese proceso.

En el caso de los guardianes en línea, la pregunta –volviendo a Kraakman– radica en cuál es el tipo de guardia que consideramos socialmente deseable. El riesgo, como señalábamos, es múltiple: una guardia desproporcionada, además de ineficiente, terminará por sacrificar actividades en línea y desconocer derechos fundamentales como la libertad de expresión y el debido proceso.

Si el intermediario asume un rol muy activo de chaperón, el impacto para la actividad en línea será manifiesto. Dependiendo del grado del incentivo que tenga para ejercer un control más o menos riguroso, el guardián comenzará a vigilar todos los rincones de su servicio en busca de contenidos indeseables, personas sospechosas o actividades simplemente riesgosas. Así como en un *shopping-mall* los guardias quieren mantener un ambiente aséptico, los inter-

---

[48] Kraakman, *supra* nota 4, p. 77. Traducción informal.

[49] Cohen, J., *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice,* Yale University Press, 2012.

mediarios en la red tratarían de mantener un servicio que no prenda ninguna alarma legal.

Aún no hemos llegado a ese estadio, en parte gracias a las inmunidades absolutas (no nos olvidemos que la mayoría de los servicios que usamos están domiciliados en Estados Unidos). Sin embargo, la protección del derecho de autor ha permeado la libertad de expresión en línea, y en este caso ni las inmunidades son absolutas ni faltan incentivos de otro tipo (económicos y políticos) para que los guardianes ejerzan un mayor control.

En este contexto los regímenes de responsabilidad no solamente llevan a los guardianes a ejercer como chaperones, sino que también puede llevarlos a que sean «bouncers», en cuyo caso la actividad de control puede quedar invisibilizada, lejos del escrutinio público. El «bouncer», recordemos, simplemente se niega de plano a admitir la entrada de la persona al bar. No quiere problemas.

Como vimos, bajo el *Communications Decency Act* los intermediarios no tienen deberes legales de diligencia. No son chaperones. Sin embargo, esto no obsta para que en los términos de referencia un intermediario prohíba la difusión de cierto tipo de contenido y establezca filtros para prevenir que algo se publique. En la Declaración de derechos y responsabilidades de Facebook, por ejemplo, el usuario acepta que no publicará «contenido que contenga lenguaje ofensivo, resulte intimidatorio o pornográfico, que incite a la violencia o que contenga desnudos o violencia gráfica o injustificada».[50]

El filtrado de contenidos en Internet no es nuevo,[51] y algunos autores lo ven como la alternativa en el horizonte para el problema de la responsabilidad de los intermediarios. Edwards lo pone en estos términos:

> «En el futuro parece que la pregunta no será si el filtrado por parte de intermediarios es posible o no, sino más bien –si es mandatorio– qué grado de precisión será necesario, qué costos se pueden imponer de manera justificada, y qué compromisos y acuerdos serán aceptables en términos de libertad de expresión, privacidad, debido proceso y barreras para el acceso al conocimiento».[52]

---

50 Facebook, «Declaración de derechos y responsabilidades», disponible en: https://www.facebook.com/legal/terms (consultada el 6 de agosto de 2013).

51 El tema se abordó parcialmente en otro documento: *Vigilancia de la red: ¿qué significa monitorear y detectar contenidos en Internet?,* en esta misma obra

52 Edwards, *supra* nota 16, p. 85. Traducción informal.

Con este futuro en ciernes el reto para muchos académicos y activistas es –siguiendo una de las críticas de Cohen– aventurase a proponer qué tipo de restricciones arquitectónicas en el entorno digital serían legítimas desde el marco de trabajo de la libertad de expresión. En otras palabras, si la idea es reivindicar este derecho hay que comenzar por explicar cómo reivindicarlo.[53]

El propósito de este documento no es plantear esa hoja de ruta (lo cual, a primera vista, es un reto enorme), pero sí, para terminar, dejar sobre la mesa una propuesta a manera de ejemplo. Regresemos a la crítica que hace Solove sobre los riesgos para la reputación y el buen nombre en línea. Podemos convenir que los discursos de odio, la difamación, el matoneo y el *character assassination,* son un problema real en Internet.[54] No obstante, un régimen de notificación y retiro –como propone Solove– atañe los mismos riesgos que hemos señalado para regímenes similares: habría un incentivo grande para censurar contenidos, el intermediario asumiría un papel de facto como juez y, posiblemente, ajustaría los términos del servicio para ejercer un mayor control. ¿Es esa la única forma de poner esa idea en práctica?

Recientemente se planteó informalmente la propuesta de que los intermediarios generaran una herramienta para que quien se considerara difamado por el contenido pudiera contrarrestarlo en el mismo sitio donde el contenido inicial apareció.[55] La idea de introducir cambios en el código informático para balancear derechos o para promover fines democráticos ha sido propuesta también por Zuckerman, Zittrain, Mayer-Schonberger y Wu, entre otros.[56]

---

[53] Cfr. Cohen, *supra* nota 49, ps. 173 y ss.

[54] Sobre este tema, ver *Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital,* en esta misma obra.

[55] Cfr. Bertoni, E., «Una solución tecnológica para el problema de la responsabilidad de intermediarios», en *Global Voices,* 30 de mayo de 2013, disponible en: http://es.globalvoicesonline.org/2013/05/30/una-solucion-tecnologica-para-el-problema-de-la-responsabilidad-de-intermediarios/ (consultada el 7 de agosto de 2013).

[56] Ver Zuckerman, E., *Rewire. Digital Cosmopolitans in the Age of Connection,* W. W. Norton and Company, 2013, pos. 3714 y ss. (versión Kindle); Mayer-Schönberger, V., *Delete: The Virtue of Forgetting in the Digital Age,* Princeton, Princeton University Press, 2009, pos. 4447 y ss. (versión Kindle); Zittrain, J., *The Future of the Internet and How to Stop It,* New Haven y Londres, Yale University Press, 2008, pos. 4447 y ss. (edición Kindle); Wu, T., «When Censorship Makes Sense: How YouTube Should Police Hate Speech», *The New Republic,* 18 de septiembre de 2012, disponible en: http://www.newrepublic.com/blog/plank/107404/when-censorship-makes-sense-how-youtube-should-police-hate-speech (consultada el 7 de agosto de 2013).

Incluso el programa de radio *On the media* del National Public Radio de Estados Unidos abrió una consulta entre sus oyentes para «arreglar» Twitter.[57]

Por supuesto, cada propuesta tiene muchos obstáculos. Ésta de la herramienta, en particular, merece varias preguntas: ¿sería una implementación requerida por ley?, ¿requeriría de la decisión de un juez?, ¿no terminaría usándose con fines políticos para acallar críticas?, ¿sería suficiente?, ¿qué pasará cuando cambien las configuraciones tecnológicas?

Bien vale la pena explorar la idea y pensar en cómo desarrollarla, sobre todo si estamos hablando de una solución tecnológica. La configuración de la red que hoy conocemos es una de tantas posibles que en medio de avatares y alternativas se fue consolidando. Y de la misma manera como se habla de una tecnología –los filtros– para restringir contenidos, bien podemos hablar de otra para promoverlos.

Un derecho de réplica en un blog o red social, o una glosa informativa en un motor de búsqueda podría desarrollarse de la manera que resulte menos extraña e invasiva para el servicio. En el caso de Twitter, *On The Media* proponía el uso de colores y banderas para advertir sobre información dudosa, agresiva o desvirtuada; en Youtube, Wu sugería un sistema de alarmas –a partir de la evaluación hecha por una comunidad de usuarios confiables– para advertir sobre discursos de odio que debían ser removidos; y en la propuesta referida se recordaba el *sidewiki* –un pestaña del navegador Chrome para hacer anotaciones sobre páginas web– que alguna vez tuvo Google. Algo similar ya tienen portales como Quartz y Medium, que permiten a los usuarios hacer comentarios en líneas o párrafos del contenido.[58]

Es imposible garantizar que estas alternativas funcionarán y desactivarán todos los posibles litigios por afirmaciones injuriosas y ataques personales. Pero implementarlas no serían del todo extrañas a uno de los fines mismos de la libertad de expresión, que es garantizar un debate equilibrado. Y tal vez la mejor manera de lograr que los intermediarios acojan soluciones como éstas

---

57 Ver «Let's Fix Twitter», *On The Media*, disponible en: http://www.onthemedia.org/blogs/on-the-media/2013/apr/26/lets-fix-twitter/?utm_source=/blogs/on-the-media/2013/may/01/lets-fix-twitter-vol-ii/&utm_medium=treatment&utm_campaign=morelikethis (consultada el 7 de agosto de 2013).

58 Cfr. Taintor, D., «Quartz Lets Readers Comment on Specific Paragraphs Atlantic Media's business brand elevates role of feedback». *Adweek.com,* disponible en: http://www.adweek.com/news/press/quartz-lets-readers-comment-specific-paragraphs-151690 (consultada el 11 de agosto de 2013).

sería mediante una mezcla de regulación y autorregulación. Es decir, leyes que ofrezcan incentivos para que los intermediarios implementen autónomamente –con algún tipo de supervisión– mecanismos tecnológicos para equilibrar estos debates de una manera transparente.

Hablar de equilibrio en materia de libertad de expresión –en palabras de Fiss– es tanto como bajarle el volumen a algunas voces y subírselo a otras.[59] Esa es una forma de ver una solución tecnológica como la expuesta. La crítica obvia a una propuesta semejante es que abrirá el camino para la censura y la imposición de contenidos. Pero tal vez una evaluación más pausada indique que podría servir para fortalecer el debate público en nuestro entorno digital.

VI. Recomendaciones

Este documento ha brindado un sustento teórico y un contexto mínimo a la discusión sobre la responsabilidad de los intermediarios en Internet. Y antes que hacer un estudio comparativo de los regímenes existentes, nos ocupamos en resaltar los puntos más relevantes de éstos para identificar los problemas y ofrecer algunos elementos de análisis. Con ese ánimo, a manera de cierre y sin excluir otros puntos señalados en el texto, hacemos las siguientes recomendaciones:

• Es importante considerar el balance entre los costos que asume el intermediario y los beneficios que obtiene por ejercer su rol de ama de llaves. Un desequilibrio entre éstos implica una estrategia fallida que además impacta negativamente actividades socialmente deseables y afecta derechos fundamentales como el debido proceso y la libertad de expresión.

• Establecer un régimen de responsabilidad objetiva para los intermediarios de Internet resulta inadecuado. Por un lado, implica imponerle obligaciones difusas a éstos, más allá de las que realmente podrían cumplir. Por el otro, se traduciría en mayores restricciones para los usuarios de Internet, en contravía de derechos y garantías fundamentales. Las decisiones judiciales en Argentina ilustran el problema de que el intermediario esté obligado a hacer juicios de valor sobre la legalidad de las acciones del usuario.

• La inmunidad condicionada parece adecuada como régimen de responsabilidad cuando establece incentivos razonables para el guardián. Es decir, cuando no le impone deberes difusos o desproporcionados de monitoreo y vigilancia. Sin embargo, en algunos modelos de inmunidad condicionada

---

59 Cfr. Fiss, O., *The Iron of Free Speech,* Harvard University Press, 1996.

–como el del DMCA de Estados Unidos– los costos que no asume el intermediario terminan en cabeza de los usuarios y la comunidad en general. En este caso los costos son vulneraciones a derechos como la libertad de expresión y el debido proceso.

• En esos términos, y sin subestimar el problema del contenido agresivo y difamatorio que pulula en la red, una inmunidad condicionada en materia de responsabilidad de intermediarios por contenidos de sus usuarios podría implicar, en la práctica, la derogación de la libertad de expresión y el debido proceso en Internet.

• Los debates sobre la responsabilidad de los intermediarios deben prestarle atención a la práctica del filtrado de contenidos, que aparece en el horizonte como una estrategia invisible para que el amo de llaves ejerza la guardia. Esto implica, de paso, empezar a mirar las condiciones que acepta el usuario cuando adhiere a los términos de referencia del servicio.

• Vale la pena explorar la idea de implementar soluciones tecnológicas –en todas sus versiones– para enfrentar los contenidos difamatorios que abundan en Internet. Particularmente, es posible pensar en adaptar un derecho de réplica a diferentes tipos de servicios y plataformas.

La tensión entre la protección de la propiedad intelectual y el intercambio de contenidos en la red. A propósito del caso Cuevana en Argentina y la «Ley Lleras» en Colombia[1]

Resumen

Este documento toma el caso de Cuevana –en el que un juez argentino ordenó el bloqueo de varias páginas de este sitio de Internet por posible violación de los derechos de autor– como punto de partida para analizar la tensión entre la protección de la propiedad intelectual y el intercambio de contenidos en la red.

Tomando como base la experiencia de los países que han liderado esta política pública, el texto señala elementos críticos para tener en cuenta, como son las restricciones previas de acceso a Internet, la proporcionalidad de las medidas y el uso de intermediarios.

El objetivo principal es que este insumo sirva como elemento de discusión para toda la región. Principalmente, se espera que en el debate de proyectos de ley sobre esta materia se analice el posible efecto negativo que puede tener para el desarrollo y uso de Internet la implementación de ciertos estándares de protección de los derechos de autor.

Este documento termina con las siguientes reflexiones:

• La protección de los derechos de autor en detrimento de derechos elementales del ciudadano, como el debido proceso y la libertad de expresión, obliga a preguntarse cuál es realmente la prioridad de los Estados en la regulación de Internet.

---

[1] Este documento fue elaborado por Eduardo Bertoni, director del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), y Carlos Cortés Castillo, investigador de la Iniciativa por la Libertad de Expresión en Internet (iLEI), con la colaboración de Atilio Grimani, asistente de investigación del iLEI.

• La presión internacional y las obligaciones contraídas en tratados internacionales sugieren que nuestra región corre el riesgo de adoptar leyes igualmente restrictivas.

• La protección de los derechos de autor, al igual que otras decisiones clave en la gobernanza de Internet, determinará en qué medida la era digital servirá para fortalecer nuestras democracias.

I. Introducción

A la luz de la tendencia internacional, las decisiones recientes contra Cuevana, el popular sitio gratuito en línea de películas y series, no resultan sorprendentes. Este caso sigue el patrón acogido por varios Estados –y apoyado decididamente por la industria del entretenimiento– de emprender una cruzada para proteger los derechos de autor en la era digital.

Más allá de si los responsables de Cuevana cometieron un delito (lo cual tendrá que probarse en el proceso penal que se les sigue), la actuación del poder judicial civil argentino permite trazar un paralelo con lo que sucede en otros países en esta materia. Igualmente, sirve para analizar la tensión entre la protección de los derechos de autor en Internet y el derecho a la libertad de expresión. Tensión que, por lo visto hasta ahora, se está resolviendo en contra de esta última.

El objetivo de este artículo es, entonces, analizar brevemente este caso –particularmente una de sus decisiones– y ponerlo en una perspectiva internacional. El propósito no es hacer un estudio comparado de legislaciones sobre derechos de autor, sino ofrecer algunos elementos iniciales de discusión para nuestra región, que apenas comienza a transitar el camino de la gobernanza de Internet.

Según reportó la BBC,[2] el 13 de marzo pasado fue arrestado en Chile Cristian Álvarez, uno de los administradores de Cuevana. Simultáneamente, un fiscal argentino abrió una causa penal contra los responsables del sitio por violación de la propiedad intelectual.[3] Sin embargo, la acción de las autoridades

---

[2] Ver «¿Llegó el fin de Cuevana?», en *BBC Mundo*, 16 de marzo de 2012, disponible en: http://www.bbc.co.uk/mundo/noticias/2012/03/120316_tecnologia_cuevana_cierre_dp.html.

[3] Sobre las consecuencias que la acción penal puede tener sobre la libertad de expresión, ver Bertoni, Eduardo, «La libertad de expresión en Internet», *La Nación*, 9 de diciembre de 2011, disponible en: http://www.lanacion.com.ar/1431250-la-libertad-de-expresion-en-internet.

venía desde antes: en noviembre de 2011, la empresa Imagen Satelital S.A. –que ostenta una licencia de Turner Internacional S.A., propietaria de varios de los contenidos disponibles en Cuevana– inició en Argentina un proceso civil contra ese sitio por el mismo motivo. Durante su desarrollo, le solicitó al juez que decretara una medida cautelar, mientras se decide el asunto de fondo, para evitar un perjuicio inminente o irreparable.

El juez argentino[4] acogió la petición de Imagen Satelital S.A. y ordenó que de manera cautelar los proveedores del servicio de conexión a Internet de Argentina (ISP, por sus siglas en inglés),[5] bloquearan el acceso a una lista de direcciones de Cuevana donde se podía acceder a las obras audiovisuales «Falling Skies», «Bric» y «26 personas para salvar el mundo». La Comisión Nacional de Comunicaciones notificó la decisión a todos los ISP del país.[6]

La solicitud de la empresa Imagen Satelital se amparó principalmente en dos normas. Por un lado, en el artículo 232 del Código de Procedimiento Civil y Comercial (CPCC) de Argentina y, por el otro, en el artículo 79 de la Ley de Propiedad Intelectual (11.723).

El artículo del CPCC establece la posibilidad de solicitar una medida cautelar cuando exista un temor fundado de que «durante el tiempo anterior al reconocimiento judicial de su derecho, éste pudiere sufrir un perjuicio inminente o irreparable». Asimismo, el artículo de la Ley de Propiedad Intelectual otorga a los jueces la facultad de decretar la suspensión de un espectáculo teatral, cinematográfico, filarmónico u analógico, o el embargo de las obras denunciadas, con el mismo fin. De esta forma, esta orden judicial no implica una atribución de responsabilidad civil.

---

4 Si bien la decisión judicial que concedió la medida cautelar emitida por el Juzgado Nacional de Primera Instancia en lo Civil N° 1, a cargo del Dr. Gustavo Caramelo Díaz, es motivo del presente artículo, se debe aclarar que esta se encuentra, a nuestro parecer, fundamentada en debida forma y no presenta rasgo de arbitrariedad alguno. Asimismo, es dable destacar que la sentencia en cuestión no se expide sobre el fondo del asunto, es decir sobre si Cuevana infringe efectivamente los derechos de propiedad intelectual, sino solo sobre la medida cautelar.

5 La sigla ISP corresponde al término Proveedores de Servicios de Internet (*Internet Service Providers*). El término se refiere únicamente a las empresas que proveen la conexión a la red. Sin embargo, en algunos contextos se usa «proveedores de servicios», que abarca todas las empresas que proveen servicios en Internet –desde conexión hasta almacenamiento de datos–.

6 Ver el anuncio de la Comisión en http://www.cnc.gov.ar/noticia_detalle.asp?idnoticia=122.

La decisión del juez tiene tres partes relevantes para el presente análisis: i) utiliza una medida cautelar para prohibir la difusión de un contenido, ii) impide el acceso de los usuarios de Internet a páginas completas de un sitio, y iii) no imparte la orden al autor del posible daño sino a unos agentes privados –los ISP– que no son responsables del contenido ni tampoco lo albergan.

Esta actuación no es extraña en el contexto internacional. A pesar de no estar amparada en una legislación específica para Internet, el juez sigue una línea muy similar a la de países como Estados Unidos o Francia, que lideran la implementación de medidas agresivas para combatir la piratería en línea. A continuación se esbozan algunos elementos de este panorama para, a partir de allí y en el contexto del Sistema Interamericano de Derechos Humanos, analizar los puntos señalados previamente.

II. Los derechos de autor en la era digital

La irrupción de Internet y la llegada de nuevas tecnologías digitales abrieron una brecha ilimitada para la creación, mezcla, copia y reproducción de contenidos. Los costos de producir información bajaron dramáticamente, mientras que el control sobre la información se volvió más complejo. El flujo de contenidos se dispersó, entre otras, a través de redes de usuarios conectados directamente (conocidas como redes de pares o *peer to peer networks* o P2P). El resultado fue la generación de una cultura digital que se caracteriza por la interconexión, la descentralización y la ausencia de control.[7]

Este escenario también abrió nuevas fronteras para «el delito y la piratería». Este último punto, en especial, llevó a muchos grupos de interés a promover la actualización de la protección de la propiedad intelectual, que está inmersa en una compleja red de tratados internacionales, acuerdos bilaterales y leyes nacionales.[8]

---

[7] Ver, entre otros, Benkler, Y., *The Wealth of Networks. How Social Production Transforms Markets and Freedom,* Yale University Press, New Haven y Londres, 2006. Capítulo 7, «Emergence of the Networked Public Sphere», p. 212.

[8] No es el objetivo de este artículo explicar este marco normativo. Baste señalar que la Organización Mundial de Propiedad Intelectual (WIPO, por sus siglas en inglés), es la agencia de las Naciones Unidas que administra la mayoría de tratados sobre propiedad intelectual. Uno de los tratados clave es el Acuerdo sobre los aspectos de los derechos de propiedad intelectual (TRIPS, por sus siglas en inglés). Otro, que se menciona más adelante en el texto, es el Acuerdo Comercial Antifalsificación (ACTA, por sus siglas en inglés).

Para muchos críticos, entre ellos Lawrence Lessig, la protección de la propiedad intelectual, en términos de hoy, es desproporcionada y económicamente ineficiente.[9] Además, amenaza de muerte la innovación digital y la naciente sociedad de la información:

> «Esta no es una situación de los derechos de autor imperfectamente protegidos; esta es una situación de derechos de autor fuera de control. A medida que millones [de personas] mueven sus vidas al ciberespacio, el poder de los dueños de los derechos de autor para monitorear y controlar el uso de "su" contenido, solo aumenta. Esto aumenta, a su vez, el beneficio de los titulares de estos derechos, pero, ¿con qué beneficio para la sociedad y a qué costo para los usuarios ordinarios?».[10]

Al enfrentarse a una realidad en que todo contenido digital es susceptible de copiarse (con las mismas características del original), el sistema de control tradicional –donde la copia de un archivo desencadena la protección de los derechos de autor– se torna inconsecuente.[11]

Antes de Internet, por ejemplo, leer un libro no estaba regulado por la ley de derechos de autor, puesto que dicho uso no implicaba la generación de copias (podía tratarse, simplemente, de un libro prestado entre amigos). Por ende, nadie tenía la necesidad de recurrir a lo que se conoce como el «uso justo»[12] para defender su derecho a leer un texto una o varias veces. Esta situación comenzó a cambiar desde el momento en que el código –la programación– de los contenidos digitales permitió que el dueño de los derechos de autor ejerciera un control directo sobre cada copia de su trabajo.

El fenómeno que quizá más preocupa a quienes lideran la lucha contra la piratería es el de las redes de pares (P2P), donde los usuarios se conectan entre

---

[9] Sobre el problema de la ineficiencia económica en la regulación de la propiedad intelectual ver, por ejemplo, Patry, W., *How To Fix Copyright,* Oxford University Press, y Palfrey, J., *Intellectual Property Srategy,* The MIT Press Essential Knowledge Series.

[10] Lessig, L., *The Future of Ideas: The Fate of The Commons in a Connected World. A Knopf E Book,* Vintage Books, pos. 3844 (edición Kindle). Traducción informal.

[11] Ver Lessig, L., *Por una Cultura Libre: Cómo los grandes grupos de comunicación utilizan la tecnología y la ley para clausurar la cultura y controlar la creatividad,* trad. de Antonio Córdoba/elástico.net, Traficantes de Sueños, Madrid, 2005, ps. 49 y ss.

[12] Lessig se refiere al «uso justo» al hablar de usos de material protegido sin autorización del titular. Se consideran «justos», y son legales sin que importe la opinión del dueño, usos de material para crítica o información periodística, entre otros. Ver Lessig, *supra* nota 11, ps. 116 y ss.

sí y comparten todo tipo de archivos.[13] En general, las P2P son consideradas por la industria del entretenimiento como santuarios para la piratería. Por lo tanto, muchos esfuerzos legales están encaminados a bloquear estas redes.

Lessig ofrece una clasificación de los tipos de contenidos que comparten los usuarios en las P2P: i) algunos descargan los archivos en lugar de comprarlos, ii) otros los descargan para «probarlos» –como una canción recomendada por un amigo– antes de comprarlos, iii) unos más descargan material protegido que ya no está a la venta –una canción de la infancia, por ejemplo– o cuyos costos de transacción resultan demasiados altos (el disco físico existe, pero está en una discotienda en una ciudad lejana), y, por último, iv) están quienes descargan contenido que no tiene derechos de autor o cuyas licencias fueron abiertas por sus titulares.[14]

Desde el punto de vista legal, argumenta el autor, solo el último grupo estaría claramente amparado. Sin embargo, de los tres restantes solo el primero puede representar un perjuicio real para el dueño del material protegido. Sin tomar en cuenta estos matices, la lucha por la protección de la propiedad intelectual se ha centrado en coartar la existencia misma de las P2P. Al igual que sucede con el caso del libro digital, en este también se pierde el equilibrio entre la necesidad de garantizar ingresos a los autores y, a la vez, el propósito colectivo de fomentar el desarrollo de nuevas tecnologías y de prácticas novedosas en las redes digitales.

Para poner en cintura a los usuarios, la idea inicial de muchos reguladores fue responsabilizar a los ISP y prestadores de servicios por el contenido que terceros transmitían a través de su red u hospedaban en sus servidores. Este enfoque no solo aplicaba para los problemas de propiedad intelectual sino también para combatir delitos en Internet como la pornografía infantil.

Esta opción fue desechada inicialmente en Estados Unidos, país precursor en la protección de la propiedad intelectual. Las ISP y la industria naciente de Internet se defendió diciendo que asumir la responsabilidad por actos ilegales de los que no tenían conocimiento, los obligaba a monitorear sus servicios permanentemente, lo cual «no solo interfería con la privacidad del usuario y

---

[13] El ejemplo inicial más conocido de P2P fue Napster, que facilitaba la conexión entre usuarios con archivos de música. El portal de Napster no guardaba los archivos de las canciones, sino que servía para ubicar el nombre de éstos y conectarse con el computador que los alojaba.

[14] Lessig, *supra* nota 11, ps. 87 y ss.

la libertad de expresión entre otras, sino que también aumentaría dramáticamente los costos de acceso a Internet».[15]

La alternativa fue ofrecerle a los ISP una especie de inmunidad legal por posibles violaciones de derechos de autor cometidas por los usuarios de sus servicios, siempre y cuando cooperaran. Con algunas variaciones, este es el enfoque que ha imperado en leyes nacionales y tratados. Como veremos a continuación, se trata de una aproximación que protege prioritariamente a los titulares de los derechos de autor, y pone en un segundo plano los derechos del ciudadano que usa Internet.

II.A. La notificación para remover contenidos en Estados Unidos

En Estados Unidos, la Ley de derechos de autor del milenio digital o DMCA por sus siglas en inglés (*Digital Millennium Copyright Act*) fue expedida en 1998. La DMCA es una ley extensa que abarca varios temas de propiedad intelectual, pero para los fines de este artículo vale la pena destacar las provisiones sobre los denominados «puertos seguros» (*safe harbors*).

La DMCA establece que un prestador de servicios de Internet[16] está exento de responsabilidad por violaciones de los derechos de autor si los contenidos que supuestamente los infringen cumplen cualquiera de estas condiciones: i) son copias incidentales de datos hechas durante la transmisión digital a favor de los usuarios, ii) es información almacenada por los usuarios, a menos que el prestador de servicios reciba una notificación de violación de derechos de autor y no investigue los cargos y remueva el material violatorio, y iii) es contenido almacenado en el caché para ofrecer un servicio más rápido o como información para herramientas de búsqueda (motores de búsqueda, por ejemplo), que eventualmente pueden conectar a los usuarios con material violatorio.

La notificación de la que trata el segundo punto es un proceso directo entre el titular de los derechos de autor y el prestador del servicio (el usuario no tiene mayor relevancia). Si el primero considera que el segundo alberga un material que vulnera los derechos de autor (por ejemplo, un video en Youtu-

---

[15] Traducción libre de A. Reichman, Jerome H., *et al.*, «Reverse Notice and Takedown Regime to Enable Pubic Interest Uses of Technically Protected Copyrighted Works», 22 *Berkeley Tech. L. J.,* 981, 2007, p. 989.

[16] Recordemos que incluye también a los ISP.

be), lo notifica formalmente. El titular del material no debe acreditar la vulneración de manera exhaustiva sino simplemente afirmar de buena fe que considera tal uso ilegal.[17]

El proveedor del servicio tampoco debe verificar la información a fondo: para mantenerse en el «puerto seguro» que ofrece la ley –es decir, para no responder secundariamente por la posible vulneración–, simplemente debe remover el contenido. Y entre más rápido lo haga mejor: hospedar contenido después de haber sido notificado de que éste puede vulnerar derechos de autor, podría comprometer su responsabilidad.[18]

El usuario, por su parte, dispone de una contranotificación para solicitar que el contenido vuelva a estar disponible en línea. Esta contranotificación debe incluir una declaración juramentada de que la remoción fue errónea y una explicación (por ejemplo, el usuario alega que está usando el material sujeto de derechos de autor dentro de los usos razonables o *fair use*).[19] El proveedor de servicios dispone de entre 10 y 14 días para resolver la solicitud. Solo después, el usuario puede intentar una demanda contra el titular de un derecho de autor que inició sin fundamento la acción para desmontar un contenido.

II.B. Los tres *strikes* en Francia

Otras leyes nacionales siguen un esquema similar. La Ley de creación e Internet, o «ley Hadopi», en Francia, expedida en 2009, creó el organismo con el mismo nombre[20] que se encarga, entre otras actividades, de administrar el sistema de los tres *strikes*. Según éste, un usuario que esté haciendo uso de contenidos protegidos por derechos de autor dispone de tres oportunidades antes de ser sancionado. En un primer correo electrónico, se le informa al

---

17 Ver sección 202 del DMCA, disponible en: http://w2.eff.org/IP/DMCA/hr2281_dmca_law_19981020_pl105-304.html.

18 «La amenaza de responsabilidad secundaria induce a los proveedores del servicio a cumplir con la previsión del DMCA sobre notificación y desmonte». Traducción libre de Seltzer, W., «Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment», *Harvard Journal of Law and Technology*, Vol. 24, Nº 1, Fall 2010, p. 177.

19 Los usos razonables incluyen, entre otros, el uso de material protegido para comentarlo, criticarlo o informar periodísticamente sobre él.

20 *Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet.*

usuario (identificado a través de su dirección IP) de la queja presentada en su contra por el titular de un material protegido. Desde ese momento el ISP (referido en este caso únicamente a los proveedores de la conexión a Internet) comienza a monitorear su conexión.

Si dentro de los seis meses siguientes, el Hadopi, el ISP o el titular del derecho de autor sospecha que el usuario está reincidiendo en la supuesta violación, se le hace llegar una carta certificada con el reclamo. Y si esta segunda advertencia no funciona, nuevamente a instancias de cualquiera de los tres actores, el ISP procede a suspender la cuenta del usuario por un lapso de entre dos meses y un año. Adicionalmente, el usuario entra a una lista negra, que implica que ningún otro ISP puede proveerle conexión a Internet. Solo en esta última etapa el usuario dispone de un recurso de apelación, en el que tiene que demostrar que no vulneró los derechos de autor.

La regla de los tres *strikes* también está prevista en la Ley de Economía Digital (*Digital Economy Act*) aprobada en el Reino Unido en 2010 pero aún pendiente de implementar por parte de la Oficina de Comunicaciones (Ofcom), el ente regulador del sector.[21]

II.C. La cooperación de las ISP en el tratado ACTA

El Acuerdo Comercial Antifalsificación (ACTA, por sus siglas en inglés), firmado en 2011 por seis países pero aún sin ratificar, establece un marco general para combatir la piratería. En relación con los derechos de autor en Internet, abre la ventana para que los prestadores de servicios de Internet y los titulares de los derechos de autor establezcan una cooperación directa entre sí, sin que sea necesaria la decisión previa de un juez.

Entre otros, el tratado exhorta a los Estados parte para que obliguen a los prestadores de servicios de Internet a entregar de manera expedita a los titulares de derechos de autor cualquier información que requieran para identificar usuarios que puedan estar vulnerando sus derechos. Igualmente, exhorta a los Estados parte a garantizar recursos expeditos que inhiban futuras vulneraciones de los derechos de autor.

En los meses recientes, la posible ratificación de este tratado por parte de la Unión Europea ha causado protestas en todos los países del continente.[22]

---

21 La implementación de esta ley ha sido objeto de múltiples debates en el Reino Unido. Algunos detalles en http://www.guardian.co.uk/technology/digital-economy-act.

22 Ver http://www.guardian.co.uk/technology/2012/jan/27/acta-protests-eu-states-sign-treaty.

La organización civil Grupo Derechos Abiertos (*Open Rights Group*) adelanta una campaña en contra de su ratificación en el Reino Unido. Según este grupo, el tratado contiene «definiciones excesivamente amplias, duras medidas punitivas y una falta de validez democrática», por lo cual es peligroso para la libertad de expresión y la privacidad en Internet.[23]

II.D. Los proyectos de SOPA y PIPA

En Estados Unidos se discuten dos proyectos de ley similares: la Ley de cese a la piratería en línea, o SOPA (*Stop Online Piracy Act*), y la Ley para proteger direcciones IP, o PIPA (*Protect IP Act*). En esencia, estos proyectos tienen el propósito de que las direcciones IP de los sitios de Internet que suministran contenido pirata pierdan su sistema de nombre de dominio o DNS (*Domain Name System*). Todos los sitios a los que se accede desde un navegador cuentan con una dirección IP compuesta por números (por ejemplo, 216.27.61.137); esta dirección se asocia a un nombre, que es el que usualmente conoce el usuario (por ejemplo, www.google.com).

Al separar el DNS de la dirección IP, la orden tradicional (teclear «google.com» y oprimir «enter» en el navegador) no funcionará. En cambio, la solicitud será enrutada a una página en la que el usuario se enterará de que el contenido al que está tratando de acceder alberga contenido violatorio de los derechos de autor y fue objeto de dicha sanción.

Esta medida se complementaría con una serie de prohibiciones para que los buscadores no puedan enlazar sus búsquedas a cierto sitios y para que los compañías de publicidad o de pagos en línea no puedan hacer negocios con ellos.

SOPA fue objeto de un rechazo considerable en Estados Unidos. Además de organizaciones civiles, intermediarios como Google y Wikipedia protestaron con franjas negras o desconexión temporal de sus sitios.[24]

II.E. Incorporación del Tratado de Libre Comercio en Colombia

El pasado 22 de marzo, el Congreso colombiano aprobó en primer debate un proyecto de ley sobre derechos de autor. Éste implementará algunas de las

---

23 Ver Stop ACTA en http://www.openrightsgroup.org/campaigns/stopacta.

24 Ver, entre otros, http://www.washingtonpost.com/politics/sopa-protests-to-shut-down-web-sites/2012/01/17/gIQA4WYl6P_story.html, y http://www.guardian.co.uk/technology/gallery/2012/jan/18/sopa-internet-blackout-websites.

obligaciones que el país adquirió con Estados Unidos en el Tratado de Libre Comercio, ratificado en octubre de 2011 por el Congreso norteamericano.

El proyecto avanza sin discusión ni debate en el Congreso, ya que el presidente Juan Manuel Santos solicitó un trámite de urgencia para tener lista la ley para la Cumbre de las Américas, que se llevará a cabo en Cartagena a mediados de abril. Es decir, Santos espera darle la buena noticia al presidente Barack Obama.

A grandes rasgos, el proyecto de ley sigue la línea de la legislación estadounidense en la materia: extiende el término de protección de las obras (vida del artista más 80 años y, en el caso de personas jurídicas, 70 años); extiende las prohibiciones de uso a cualquier forma de difusión, reproducción o comunicación a través de Internet (pero sin establecer claramente los criterios de uso justo), y hace igualmente extensivos a Internet los delitos en algunos tipos de violación de los derechos de autor. También recoge, casi en los mismos términos, la provisión antielusión (*anticircumvention*) que tiene el DMCA de Estados Unidos.

Al igual que las normas en que está basado, el proyecto incorpora definiciones amplias (por ejemplo, define «lucro» como la «ganancia o provecho que se saca de algo») e invierte la carga de la prueba a favor del supuesto titular del derecho.

El año pasado, el gobierno presentó un proyecto que contemplaba medidas de notificaciones de retiro de contenidos y de puertos seguros para los ISP, en términos casi idénticos al DMCA. La presión de la opinión pública hizo que la iniciativa se retirara. Este tema no ha sido incluido, de momento, en el nuevo proyecto.

III. Desproporción, intermediarios y censura previa

La aplicación de estas normas ha suscitado un amplio debate alrededor de los mismos puntos que se ven ahora en el caso de Cuevana: el uso de intermediarios, la censura previa y la proporcionalidad de las medidas.

En primer lugar, el caso de Cuevana presenta una diferencia fundamental con el mecanismo previsto en otros países. La decisión de bloquear algunas páginas de ese sitio de Internet hace parte de un proceso judicial, lo que permite a los afectados defender sus derechos con todas las garantías procesales. Esto se debe, en parte, a que no se trata de la aplicación de una norma específica para Internet como aquellas expedidas en los últimos años, que han privatizado esta labor. En la mayoría de los casos, estas regulaciones especiales han impedido que los ciudadanos cuestionen tales decisiones, que

terminan en manos de autoridades administrativas o de los propios prestadores de servicios.

Y si bien la decisión contra Cuevana se enmarca en un proceso judicial, hace uso de los intermediarios –específicamente los ISP– para bloquear el acceso a ciertos contenidos de su página. En la atmósfera de Internet, los intermediarios (conocidos como «porteros» o *gatekeepers*) son fundamentales en el proceso de difundir contenidos y, por lo tanto, ostentan el poder de restringirlos o promoverlos. En el debate público de hoy las opiniones no se oyen en la plaza pública o encima de una caja de jabón. Requieren de un intermediario.

Las provisiones del ACTA norteamericano y otras incluidas en los proyectos de las leyes SOPA y PIPA, prevén una mayor responsabilidad y mayor discrecionalidad de los prestadores de servicios en la labor de determinar, de la mano de los titulares de los derechos de autor, qué información debe ser removida de Internet. La preocupación en el caso que nos ocupa es, entonces, si la decisión del juez argentino es la cuota inicial del protagonismo que empezarán a adquirir los proveedores de Internet en estas controversias en América Latina.

> «Algunos académicos –y muchos en la industria de la publicación de entretenimiento– argumentan que los proveedores de servicios deberían actuar como guardias de los derechos de autor (…). Este análisis se enfoca en los daños a la propiedad que genera la vulneración de los derechos de autor, y tiende a minimizar los costos públicos –en reducción del discurso y falta de acceso– que conlleva el uso de intermediarios impositivos».[25]

Por otro lado, la medida cautelar que ordena el juez argentino se asemeja a la notificación para remover contenidos bajo el DMCA en Estados Unidos. En otras palabras, puede verse como una forma de censura previa. En el escenario norteamericano, el diseño de la norma crea los incentivos para que los prestadores de servicios remuevan expresiones de todo tipo –tanto legales como ilegales–[26], mientras que el ciudadano enfrenta un proceso desventajo-

---

[25] Seltzer, *supra* nota 18, p. 183. Traducción informal.

[26] Por ejemplo, en 2009, el propio académico Lawrence Lessig fue objeto de una notificación de Warner Music de retiro de contenido bajo el DMCA. El video era, precisamente, una conferencia sobre el problema de protección de los derechos de autor y el uso justo de materiales protegidos. Ver http://www.techdirt.com/articles/20090428/1738424686.shtml.

so que muchas veces termina por inhibir el interés de expresar su idea.[27] Este fenómeno se conoce como el «efecto inhibitorio» (*chilling effect*): «Disuadidos por el temor del castigo, algunos individuos se abstienen de decir o publicar algo que legalmente podrían y, de hecho, deberían [decir]».[28]

El antecedente de Cuevana puede generar el mismo efecto inhibitorio si se aplica a todo tipo de controversias donde exista una posible vulneración de los derechos de autor. Si la medida cautelar se convierte en la regla, los usuarios optarán por evitar el costo de un proceso judicial y optarán por restringir su libertad de expresión, más allá de que no pese una decisión final sobre ellos.

A la luz de la Convención Interamericana sobre Derechos Humanos parece claro que la medida previa deviene en censura previa. Según el artículo 13, el derecho a la libertad de expresión «no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley».[29]

Para un juez puede parecer justificada la medida cautelar cuando verifica que existe, por un lado, un sitio en Internet que ofrece películas gratis y, por el otro, un tercero que acredita ser el titular de los derechos sobre esos contenidos. Sin embargo, cuando ese mismo juez se enfrente a expresiones con usos parciales de esos contenidos –por ejemplo, un fragmento mezclado, una parodia o una crítica–, ¿podrá tomar la misma decisión? El riesgo que corre es resolver la duda en contra de la libertad de expresión.

Este último punto nos lleva al problema de proporcionalidad. En el caso de Estados Unidos y Francia, la carga de la prueba está invertida en contra del

---

[27] Cfr. *ibídem*, ps. 193 y ss.

[28] Schauer, F., «Fear, Risk and the First Amendment: Unraveling the Chilling Effect», *Faculty Publications,* Paper 879, disponible en: http://scholarship.law.wm.edu/facpubs/879, 1978, p. 693. Traducción informal.

[29] Adicionalmente, el numeral 4 del mismo artículo añade que «los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia", pero sin desconocer la regla anterior. En este caso parece que el juez sugiere una analogía entre Cuevana y un espectáculo cinematográfico para aplicar la ley 11.723, pero aun así no cumple con el objeto aceptado por la Convención de censurar previamente tales contenidos únicamente para proteger la moral de la infancia y la adolescencia. En parte, la contradicción entre esta norma y la Convención se explica en la diferencia de épocas: la Ley de Propiedad Intelectual es de 1933 mientras que el Pacto de San José de Costa Rica se suscribió en 1969.

ciudadano: debe ser éste el que pruebe, después de haber sido sancionado por fuera de un proceso judicial, que el contenido que colgó en un sitio de Internet no desconoce los derechos de autor de terceros. En el caso de Francia, además, el usuario puede estar desconectado de la red por orden de una autoridad administrativa y sin que medie una decisión judicial, antes de poder cuestionar legalmente tal procedimiento.

En la mayoría de los casos esas medidas son desproporcionadas. Es decir, el fin que se persigue no concuerda con la magnitud de la medida. Un video de un bebé cantando la canción de un artista conocido o un estudiante copiando en su blog un poema de su escritor favorito pueden constituir usos no permitidos por los derechos de autor. No obstante, no guardan relación con el objetivo de combatir la piratería; no representan un riesgo del que la sociedad se deba cuidar.

La desproporción también se refiere al impacto que estas medidas pueden tener en el discurso político. Durante las elecciones presidenciales de 2008 en Estados Unidos, la campaña de John McCain fue objeto de varias notificaciones de remoción de videos en Youtube. Se trataba de comerciales legítimos de la campaña en un momento clave del debate.[30]

En la Declaración conjunta acerca de Internet, los relatores de libertad de expresión de las Naciones Unidas y de la Comisión Interamericana de Derechos Humanos, y la representante de la Organización para la Seguridad y la Cooperación en Europa se refrieron a la desproporción en el punto particular del bloqueo de contenidos:

> «El bloqueo obligatorio de sitios web enteros, direcciones IP, puertos, protocolos de red o ciertos tipos de usos (como las redes sociales) constituye una medida extrema –análoga a la prohibición de un periódico o una emisora de radio o televisión– que solo podría estar justificada conforme a estándares internacionales, por ejemplo, cuando sea necesaria para proteger a menores del abuso sexual».[31]

---

30 Ver https://www.eff.org/deeplinks/2008/10/mccain-campaign-feels-dmca-sting. Seltzer menciona este ejemplo en el artículo citado de ella. Para la autora, el hecho de que este proceso del DMCA no se haga a través de las cortes evita que se desencadene un debate a luz de la Primera Enmienda, lo cual pondría sobre la mesa problemas como este.

31 Relatoría Especial para la Libertad de Expresión, comunicado de prensa R50/11, disponible en: http://cidh.org/relatoria/showarticle.asp?artID=848&lID=2.

En el caso de Cuevana, las páginas bloqueadas que contienen las series y películas supuestamente ilegales, pueden contener igualmente comentarios de usuarios o artículos de opinión sobre estos contenidos; expresiones que de ninguna manera son ilegales. Y, nuevamente, este caso puede parecer de fácil respuesta para algunos, pero a medida que lleguen otros más complicados, habrá que volver a mirar si este antecedente de bloquear páginas enteras de Internet en función de proteger los derechos de autor no es una solución desproporcionada.

IV. Conclusión

La protección de los derechos de autor en detrimento de derechos elementales del ciudadano, como el debido proceso y la libertad de expresión, obliga a preguntarse cuál es realmente la prioridad de los Estados en la regulación de Internet. En los términos planteados, la estrategia de protección de los derechos de autor implica tener «más delfines atrapados en las redes de pesca».[32] Es decir, más inocentes en el grupo de culpables. Y, aun así, la efectividad de esta estrategia es altamente discutible.

La presión internacional y las obligaciones contraídas en tratados internacionales sugieren que nuestra región adoptará leyes igualmente restrictivas.[33] A pesar de esto, no está de más abogar por una implementación que tome en cuenta los estándares de libertad de expresión. Esto es, que se aleje de la censura previa de contenidos y de medidas desproporcionadas, que no otorgue un poder arbitrario y excesivo a los intermediarios y que garantice la posibilidad de recurrir las decisiones ante un tribunal.

La protección de los derechos de autor, al igual que otras decisiones clave en la gobernanza de Internet, también determinará en qué medida la era digital servirá para fortalecer nuestras democracias.

---

32 Seltzer, *supra* nota 18, p. 180.

33 Es el caso del proyecto de ley conocido en Colombia como «ley Lleras», que incluye varias de las disposiciones contenidas en el DMCA de Estados Unidos.

Libertad de expresión versus libertad de expresión: la protección del derecho de autor como una tensión interna[1]

Resumen

Este documento explora los argumentos teóricos que sustentan el derecho de autor e intenta una aproximación distinta a las que habitualmente se exponen. Además de las razones vinculadas con el derecho de propiedad y las económicas, el *copyright* también es un desarrollo de la libertad de expresión. Y, siendo así, las tensiones que genera se vuelven realmente un pulso interno entre dos tipos de expresión –la de los titulares y la de los ciudadanos del común–. La primera parte de este documento aborda los argumentos vinculados al derecho de propiedad (argumentos «propietarios») y los económicos (argumentos «económicos»), y señala la dificultad de que éstos entren en diálogo con las visiones nuevas del derecho de autor. La segunda parte desarrolla la idea del derecho de autor como libertad de expresión y propone un ejercicio de ponderación interna entre reivindicaciones expresivas. Por último, se hacen las siguientes recomendaciones:

• Los argumentos propietarios y económicos aíslan el *copyright,* como una especie de derecho autónomo y autosuficiente. Desde allí es difícil cuestionar el impacto que tiene esta regulación en la libertad de expresión.

• Delimitar el conflicto entre *copyright* y libertad de expresión como una tensión interna entre dos expectativas válidas de expresión puede dar luces para hacer una mejor ponderación de los intereses involucrados.

---

[1] Este documento fue elaborado por Carlos Cortés Castillo, investigador de la Iniciativa por la Libertad de Expresión en Internet (iLEI), del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo, y por Eduardo Bertoni, director del CELE.

• Si se acepta que ambos lados tienen una aspiración legítima en el debate público, resulta inaceptable cualquier solución que implique que uno de ellos ceda del todo a favor del otro.

• A pesar del reto que implica un ejercicio de ponderación, es posible examinar los proyectos de ley y las leyes sobre derecho de autor de esta perspectiva. Y es necesario hacerlo sin tener una visión predefinida de cuál es la protección más importante.

• El enfoque de libertad de expresión puede dar luces para revisar normas de notificación y retiro, extensiones de términos de protección del derecho de autor, y el uso extendido de Medidas Tecnológicas de Protección.

I. Introducción

La revolución digital rompió para siempre las barreras naturales del flujo de información. Hace un par de décadas, cuando no hablábamos el lenguaje de los bits, una novela o una canción estaban inexorablemente atadas al libro o disco que las contenían. Además, era costoso y dispendioso editar imágenes o videos, mucho más remezclar y crear contenidos a partir de los existentes.

La llegada de las plataformas en línea y las aplicaciones y dispositivos digitales no solo democratizó el acceso a esta información y descentralizó el proceso creativo. También democratizó un conflicto que durante siglos estuvo restringido al círculo cerrado de casas disqueras, industrias creativas, empresas y artistas: el uso sin autorización de obras protegidas por derechos de autor.

La propiedad intelectual se refiere a las creaciones de la mente, tales como las invenciones, los trabajos literarios o artísticos, y los diseños, símbolos y nombres empleados en el comercio.[2] El derecho de autor, en particular, protege las creaciones literarias y los trabajos artísticos, y se encuentra consagrado, entre otros, en el artículo 27 de Declaración Universal de Derechos Humanos: «Toda persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora».

Este derecho suele fundamentarse teóricamente como un tipo de propiedad y como una protección necesaria para que exista creación e innovación. No

[2] Cfr. Organización Mundial de la Propiedad Intelectual, «¿Qué es propiedad intelectual?», disponible en: http://www.wipo.int/about-ip/en/index.html (consultada el 2 de diciembre de 2013).

obstante, lo que vemos en la práctica es que la innovación descentralizada en Internet se mueve por canales distintos y por razones tanto sociales como económicas. Para Lessig, en el entorno digital la economía de la creación es híbrida, ya que se construye sobre ambos tipos de motivaciones.[3] Lo cierto es que en el desarrollo de ese proceso, la expresión colectiva de blogueros, periodistas, artistas y ciudadanos del común se estrella con duras prohibiciones.[4]

En estas condiciones, es usual que el *copyright* entre en tensión con la libertad de expresión de los usuarios de Internet. «¡Bajar una canción es como robarse una cartera!», «¡Sin *copyright* no habrá innovación!», es lo que les oímos decir a los titulares de contenido, sin que las razones del lado contrario merezcan mayor atención.

El propósito de este documento es explorar esos argumentos teóricos que sustentan el derecho de autor y proponer uno distinto: como varios autores sugieren, el *copyright* también es un desarrollo de la libertad de expresión. Y siendo así, las tensiones que genera se vuelven realmente un pulso interno entre dos tipos de expresión –la de los titulares y la de los ciudadanos del común–.

La primera parte de este documento aborda los argumentos propietarios y económicos, y señala la dificultad de que éstos entren en diálogo con las visiones nuevas del derecho de autor. La segunda parte desarrolla la idea del derecho de autor como libertad de expresión y propone un ejercicio de ponderación interna entre reivindicaciones expresivas. En términos generales, se propone este enfoque como un camino para repensar los debates legislativos y judiciales en la materia.[5]

Este documento se alimenta mayoritariamente de la teoría norteamericana sobre el *copyright* y la libertad de expresión, que si bien tiene como referente

---

[3] Cfr. Lessig, L., *Remix. Making Art and Commerce Thrive in the Hybrid Economy,* Bloosmbury, 2008.

[4] Diversas organizaciones han propuesto acercamientos alternativos. Ver, entre otros, Fundación Vía Libre, *Argentina Copyleft. La crisis del derecho de autor y las prácticas para democratizar la cultura*, Busaniche, B. Ed. Heinrich Böll Stiftung, 2010; Artículo 19. El Derecho a Compartir: Principios de la Libertad de Expresión y los derechos de propiedad intelectual en la Era Digital, Colección de Normativa Internacional, 2013.

[5] La idea de este documento surgió después de que el *Centre for Law and Democracy* presentara en el CELE en Buenos Aires, en junio pasado, el documento «Reconceptualizando los derechos de autor: estableciendo un esquema consistente con la libertad de expresión en la era digital» (referido en detalle más adelante).

la Primera Enmienda de Estados Unidos, sirve para plantear un debate útil en nuestra región. Más aún si tenemos en cuenta que ese país viene «exportando», a través de negociaciones bilaterales, algunas de sus normas en este tema.

I.A. Los argumentos propietarios y económicos en el derecho de autor

El derecho de autor –y la propiedad intelectual en general– suele justificarse teóricamente en términos de un desarrollo natural del derecho a la propiedad.[6] Varios autores[7] ubican este fundamento en John Locke, para quien cada hombre tiene «una propiedad que pertenece a su propia persona; y a esa propiedad nadie tiene derecho, excepto él mismo. El trabajo de su cuerpo y la labor producida por sus manos podemos decir que son suyos».[8] En consecuencia, cualquier creación –una canción o un texto y, últimamente, un programa de computación– es el resultado de un esfuerzo de un individuo y, por lo tanto, no es de nadie más sino de él.[9]

Antes que de origen natural, para Heitinger, la conceptualización de la creación intelectual como propiedad es utilitaria: materializa la idea liberal de la autonomía individual.[10] En una línea similar, Epstein considera que el desarrollo de derechos propietarios es el resultado de la maximización de la utilidad para nuestras instituciones políticas y sociales.[11] Drahos y Braithwaite,

---

[6] En estricto sentido, *copyright* y «derecho de autor» no son sinónimos: mientras el primero se centra en las condiciones de uso y comercialización de una obra, el segundo incluye también el reconocimiento de la autoría de la obra, más allá de que esté en poder de terceros. Para los efectos de este documento, los términos se usan como sinónimos.

[7] Zimmerman, Diane, «Information as Speech, Information as Goods: Some Thoughts in Marketplaces and the Bill of Rights», *William and Mary Law Review*, vol. 33, Nº 3, artículo 3, 1992.

[8] Locke, J., *Segundo tratado sobre el gobierno civil. Un ensayo acerca del verdadero origen, alcance y fin del gobierno civil,* Colección Clásicos del Pensamiento, Tecnos, 2006, num. 27, p. 34.

[9] Ver, entre otros: op. cit., p. 707; Mayer-Schönberger, V., «In Search of the Story: Narratives of Intellectual Property», *Virginia Journal of Law and Technology*, vol. 10, Nº 11, 2005; Hettinger, E., «Justifying Intellectual Property», *Philosophy & Public Affairs,* vol. 18, Nº 1, 1989, ps. 31-52.

[10] Cfr. Hettinger, *supra* nota 8.

[11] Cfr. Epstein, en Mossoff, A., «Is Copyright Property?», *San Diego Law Review,* vol. 42-2005, 2010, p. 33.

por su parte, afirman que, más allá de la retórica de la creación y el trabajo, la propiedad intelectual era una necesidad en la agenda de comercio de Europa a partir del siglo XVIII.[12]

La afirmación de que la creación es el fruto del trabajo individual ha sido cuestionada en su esencia misma: «¿Qué porción del valor de escritos, invenciones e información de negocios es atribuible al obrero intelectual?», se pregunta Heitinger.[13] Desde esta perspectiva, la creación individual es fundamentalmente un producto social. Al inventor lo precedieron otras personas con ideas relacionadas y productos similares, y su proceso creativo estuvo mediado por toda serie de influencias externas. En resumen, a la hora de determinar la autoría el único factor relevante no puede ser el trabajo del autor final.

La respuesta del lado opuesto pasa, precisamente, por no subestimar esa labor final: «Es posible ubicar en una persona, o en un grupo pequeño de autores conjuntos, la chispa creativa o el duro esfuerzo que implicó tomar esas influencias dispersas y fusionarlas en un trabajo coherente, merecedor de nuestra atención»,[14] dice Epstein. Sin el creador solo habría ideas sueltas; sin el creador no habría producto.

De cualquier forma, el argumento propietario, ya sea desde una perspectiva naturalista o meramente liberal, se ha consolidado con el tiempo y es la narrativa dominante del derecho de autor, con amplia acogida –por distintas razones– entre legisladores y jueces.[15] Y al ser la piedra de toque, es también el terreno que disputan los contradictores del régimen actual. Para ellos, el *copyright* no es una forma de propiedad o, en el peor de los casos, es una propiedad disminuida.

«La ley que protege mi derecho de autor lo hace de una manera más limitada que la ley que protege mi carro (…) Yo no tengo derecho a usar tu carro; yo sí tengo derecho a hacer un uso justo de tu libro», afirma Lessig.[16] Parece

---

12 Cfr. Drahos, P. y Braithwaite, J., *Information Feudalism. Who Owns the Knowledge Economy?,* The New Press, Nueva York, 2002.

13 Hettinger, *supra* nota 8, p. 37. Traducción informal.

14 Epstein, R., «Liberty versus Property? Cracks in the Foundations of Copyright Law», *John M. Olin Law & Economics,* Working Paper Nº 204, 2004, p. 29. Traducción informal.

15 Cfr. Mayer-Schönberger, *supra* nota 8, y Zimmerman, *supra* nota 6.

16 Lessig, L., *The Future of Ideas: The Fate of the Commons in a Connected World,* Random House, Vintage, 2002, Loc. 3930, 3932-3933 (edición Kindle).

claro que las reglas de la propiedad real no aplican a la propiedad intelectual. El derecho que se tiene sobre un bien real es perpetuo mientras que el que se tiene sobre una creación es limitado. La ley no protege ideas sino expresiones y tiene que dejar un espacio para los usos justos (*fair use*) de materiales protegidos. La propiedad intelectual –concluye Lessig– pone en la balanza la protección de la propiedad y otros intereses.

En este enfoque, las creaciones intelectuales protegidas se contraponen a las creaciones comunes, que al no tener protección –bien sea porque expiró o no se exigió– hacen parte de la bolsa colectiva de la sociedad. Al exigir que se reduzca el alcance del *copyright,* lo que Lessig y otros intelectuales buscan, entre otras cuestiones, es que esa bolsa común, ese *commons,* sea más robusta para descentralizar y fortalecer la creación y la innovación.[17]

Sin embargo, el riesgo de hablar de bienes comunes es que implica aceptar la premisa de la propiedad. Desde el mismo bando de Lessig, Vaidhyanathan planteó el problema: «Cometemos un grave error cuando escogemos engancharnos en discusiones sobre copyright en términos de "propiedad" como se entiende comúnmente. El copyright es un monopolio otorgado por el Estado por razones particulares de política pública».[18]

Quienes defienden el argumento propietario consideran errado tanto el intento de Lessig de hablar de una «propiedad disminuida» como el de Vaidhyanathan de otorgarle un estatus meramente legal. Frente a esto último, Mossoff afirma que al final de cuentas toda propiedad deviene de la regulación; la propiedad es un monopolio particular para cada persona.[19] Y en relación con la tensión que plantea Lessig, Epstein dice que el hecho de que el derecho de autor riña con otras libertades no desdice de su condición de propiedad. Para él, la propiedad en general entra en conflicto con otras libertades, y no por ello pierde su esencia.[20]

---

[17] Ver, además de Lessig, Tushnet, R., «Copy This Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It», *The Yale Law Journal*, 114(3), 2004; Karaganis, J., «Rethinking Piracy», en *Social Science Research Council,* Media Piracy in Emerging Economies, 2011; Benkler, Y., *The Wealth of Networks*, Yale University Press, New Haven y Londres, 2007; Drahos y Braithwaite, *supra* nota 11.

[18] Vaidhyanathan, en Mossoff, *supra* nota 10, nota 20.

[19] Cfr. Mossoff, *supra* nota 10.

[20] Cfr. Epstein, *supra* nota 13, p. 29. Traducción informal.

Al hablar de un monopolio otorgado por el Estado, Vaidhyanathan está apuntando hacia el otro fundamento que tiene el derecho de autor –que él parece encontrar más apropiado para rebatir–, y es el económico. Éste no es excluyente con el argumento propietario, pero sí tiene una naturaleza distinta: las creaciones intelectuales se protegen mediante un monopolio temporal a favor del autor para que éste recupere la inversión y privatice los frutos de la explotación de la obra. Como garantía previa a la creación es, además, un incentivo para que haya producción intelectual.

Este planteamiento se basa en la característica abierta y no-rival de las creaciones intelectuales. Una canción o un libro, por ejemplo, son bienes públicos en un sentido económico: mi consumo no agota el bien y es posible que otras personas lo consuman sin que necesariamente lo hayan adquirido. Así, el *copyright* –al establecer barreras de acceso y uso– sirve el propósito de ayudar al autor a apropiarse del valor de la creación, que de otra manera estaría disponible para que otros la tomaran.[21]

Decíamos que el argumento económico no está lejos del propietario. Son varias las razones, pero ilustrémoslo acá en los términos de Posner y Landes: «La teoría económica de derechos propietarios enfatiza no solamente sus efectos en términos de incentivos, es decir, la inversión que alienta, sino también su efecto optimizador en usos actuales de la propiedad».[22] Sin estar defendiendo una visión tradicional del argumento propietario, Posner y Landes sí ofrecen una respuesta relevante a la idea de que entre más creaciones intelectuales pasen al dominio común, mejor. Para ellos, sin un derecho de dominio sobre la obra se corre el riesgo de que ésta pierda su valor por exceso de uso.

Los autores usan el ejemplo de Mickey Mouse. A lo largo de todos estos años el titular –Disney– ha cuidado la obra de una sobrexposición y mal uso. Si pasara al dominio común (lo cual ha evitado con esmero el *lobby* de esa empresa), rápidamente estaría asociada a todo tipo de causas y productos. En poco tiempo el personaje estaría quemado y el público, aburrido.[23] Habría perdido todo su valor y utilidad para la sociedad.

---

[21] Cfr. Rothchild, J., «The Social Costs Of Technological Protection Measures», *Florida State University Law Review*, vol. 34, 2007, ps. 1181-1220.

[22] Posner, R. y Landes, W., «Indefinitely Renewable Copyright», *John M. Olin Law & Economics,* Working Paper Nº 154, 2002, p. 12. Traducción informal.

[23] Cfr. Posner y Landes, *supra* nota 21, ps. 11 y ss.

A partir de esto, Posner y Landes proponen que el *copyright* sea renovable de manera indefinida, pero no automática ni predeterminada para todas las creaciones. Esto, en teoría, protegería las obras económicamente eficientes y dejaría en el dominio público la mayoría restante, sobre las cuales sus propietarios no tienen expectativa económica (valga la pena añadir que la idea de un derecho de autor renovable ha sido planteada también por Lessig).[24]

Muy en la línea de la teoría económica a la que pertenece, el análisis de Posner y Landes deja de lado los puntos que desbordan ese marco conceptual. Elementos como el impacto social del acceso a obras, la descentralización de la innovación y los incentivos no financieros que impulsan la creatividad, quedan fuera de la ecuación. Elementos que, además, tienen una mayor vigencia en el entorno digital.

Para quienes abogan por un sistema de derecho de autor más equilibrado, los argumentos propietarios y económicos constituyen una muralla infranqueable. Por un lado, la justificación propietaria ubica las creaciones intelectuales en el mismo nivel de una finca o un lote –las metáforas en esta narrativa son muy importantes–, donde los usos permitidos son como senderos para el paso público o servidumbres para el agua: la excepción antes que la regla. Por el otro, la justificación económica reduce el proceso creativo y la autoría a una ecuación racional de transacciones.

Los derechos de terceros sobre las creaciones intelectuales privadas no parecen entonces tener contrapeso alguno. Al contrario, si el objetivo es maximizar la producción para el consumo público y sacar el mejor provecho de este tipo de propiedad, la frontera puede moverse hacia adelante sin mayores reparos. Bajo este razonamiento, cualquier expansión del derecho de autor es defendible.[25] Según Zimmerman, sin mejores principios para limitar esta esfera, «el resultado probable es que más y más porciones de la actividad comunicativa caerán en el lado propietario».[26]

Algunos podrían decir –siguiendo a Vaidhyanathan– que en el campo exclusivamente económico es posible encontrar un equilibrio. Es decir, que es

---

[24] Cfr. Lessig.

[25] Cfr. Zimmerman, *supra* nota 6, p. 704.

[26] Zimmerman, *supra* nota 6, p. 673.

posible delimitar el nivel deseable de protección del *copyright* si se determina empíricamente el valor que debe obtener el autor por la creación (que incluya la inversión y la retribución). Por fuera de ese umbral, la protección se tornaría ineficiente. No obstante, «es difícil, sino imposible, determinar con algún nivel de precisión la extensión de copyright que conduciría a un nivel óptimo de respaldo a la autonomía creativa y que simultáneamente permita un acceso suficiente para el usuario».[27]

En medio de este pulso inclinado, el término de protección del derecho de autor se ha venido extendiendo paulatina y sostenidamente en leyes nacionales y tratados internacionales,[28] mientras que los derechos conexos se han expandido. Particularmente, esta colección de derechos emanados del *copyright* está «canibalizando» sobre el camino los valores de libertad de expresión ubicados en el otro lado de la balanza.[29] Leyes como el *Digital Millennium Copyright Act* establecen mecanismos de censura previa a favor de cualquier sospecha de infracción al derecho de autor.[30] Igualmente, las Medidas

---

[27] Netanel, en Rotchild, cita 114. Traducción informal.

[28] El caso de Estados Unidos es paradigmático, y se refleja en legislaciones en todo el mundo: en 1790, el término del *copyright* era de 14 años con posibilidad de renovación por el mismo periodo; el término inicial fue extendido a 28 años en 1831; la renovación fue ampliada igualmente a 28 años en 1909, y a 47 años en 1962; en 1976, el *Copyright Act* cambió la fórmula a la vida del autor más 50 años, que en 1998 se extendió a 70.

Sobre los derechos conexos y las Medidas Tecnológicas de Protección, ver Rothchild, *supra* nota 20, y Cohen, J., «Pervasively Distributed Copyright Enforcement», Georgetown Public Law and Legal Theory Research, Paper Nº 892623, *The Georgetown Law Journal*, vol. 95:1, 2006.

[29] Cfr. Zimmerman, *supra* nota 6, p. 666.

[30] Diversos autores consideran que el diseño de incentivos y presunciones de esta ley favorece el control previo de contenidos. Esto se ha traducido, en la práctica, en que contenidos legítimos de interés publico resulten retirados de la red. Ver, entre otros, Nunziato, C., «Preservar la libertad en Internet en las Américas», en Bertoni, E. (comp.), *Hacia una Internet libre de censura. Propuestas para América Latina*, Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Facultad de Derecho, Universidad de Palermo, 2012, ps. 11-45; Seltzer, W., «Free Speech Un-moored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment», *Harvard Journal of Law and Technology,* vol. 24, Nº 1, Fall 2010, ps. 171 y ss.; von Lohman, F., *Unintended Consequences: Twelve Years Under The DMCA,* Electronic Frontier Foundation, 2010.

Tecnológicas de Protección son la punta de lanza para que los titulares amplíen el control sobre sus contenidos, lo cual impide usarlos incluso con propósitos legales –tales como la denuncia periodística o la parodia–.[31]

En Estados Unidos –que sirve como guía para la discusión de este documento–, *copyright* versus libertad de expresión ha sido siempre una proposición perdedora para esta última. O, como dice Rubenfeld, la regulación de *copyright* en ese país ha sido una enorme zona de *duty-free* para la aplicación de la Primera Enmienda.[32] Subido en los hombros de los argumentos propietarios y económicos, el *copyright* se erige como un derecho independiente (garantizado en la Cláusula Octava de la Constitución) cuyos contornos pueden ser expandidos por el Congreso atendiendo los propios fines de este derecho. Una especie de argumento circular en el que la libertad de expresión no tiene cabida.[33]

II. El ejercicio interno de ponderación. Distribución de oportunidades de expresión

Para hacer este ejercicio de «rebalanceo» es necesario abordar la libertad de expresión desde su acepción colectiva, de la cual Fiss es quizá el mejor exponente. Si bien su planteamiento está hecho alrededor de la Primera Enmienda norteamericana, bien puede extrapolarse a una teoría general sobre los valores que alimentan este derecho. Partiendo de allí será más fácil ilustrar la tensión entre el *copyright* y la libertad de expresión como un pulso interno; como un dilema entre dos derechos de igual entidad.

Según la teoría democrática de la libertad de expresión que defiende Fiss, este derecho tiene preeminencia en las cartas políticas no porque garantice una forma de autoexpresión o autorrealización, sino porque es fundamental para

---

31 Cfr. Cortés Castillo, C., *Mirar hacia el norte es mirar hacia atrás: el impacto negativo de la DMCA. El mecanismo de notificación y retiro y las Medidas Tecnológicas de Protección*, Fundación Karisma, Documentos 2, julio de 2013, disponible en: http://karisma.org.co/wp-content/uploads/2013/07/Paper2ImpactoNegativoDMCA.pdf (consultada el 5 de diciembre de 2013).

32 Cfr. Rubenfeld, en Horowitz, Steven, «A Free Speech Theory of Copyright», *Stanford Technology Law Review,* 2009, nota 21.

33 Cfr. Corte Suprema de Estados Unidos, *Eldred vs. Ashcroft*, 537 US 186, 2003. Ver el análisis de la decisión en Horowitz, *supra* nota 31.

la autodeterminación colectiva. Esta teoría se construye en oposición a la tradicional liberal (o libertaria) que subraya el derecho inalienable de cualquier persona a expresarse libremente sin importar el contenido o los fines. Es, simplemente, una manifestación de la autonomía individual. Para Fiss, esta aproximación no es suficiente para explicar por qué suelen primar los derechos de quienes se expresan sobre los de aquellos que están aludidos en esas expresiones o que tienen que escucharlas.[34]

Esto último puede ilustrarse con la Convención Interamericana sobre Derechos Humanos. El numeral segundo del artículo 13 dispone que el derecho a la libertad de expresión «no puede estar sujeto a previa censura sino a responsabilidades ulteriores», que deben estar fijadas por ley y ser necesarias para garantizar los derechos o reputación de los demás, la seguridad nacional, el orden público o la salud y moral públicas. Así, una información que por ejemplo vulnere la intimidad o el buen nombre de una persona verá la luz pública antes que sobre ella pueda ejercerse algún control.

Que la libertad de expresión sea un derecho colectivo –de realización individual– le impone al Estado obligaciones más allá del clásico deber de no interferir en la divulgación de ideas e informaciones. «No interferir» y «no hacer» se quedarían cortos en el propósito estatal de asegurar un debate público robusto, desinhibido y abierto. Fiss lo pone en los siguientes términos:

> «El Estado puede tener que actuar para fomentar el debate público en circunstancias en que poderes por fuera del Estado estén sofocando la expresión. Puede tener que asignar recursos públicos –distribuir megáfonos– a aquellos cuyas voces no serían oídas de otro modo en la plaza pública. Puede tener incluso que silenciar las voces de unos para que se oigan las voces de los otros».[35]

El Estado puede «distribuir megáfonos» de distintas formas. Goodman lo llama «redistribución de expresión» a través de políticas públicas, y ofrece los siguientes ejemplos: la regulación que limita la propiedad de sistemas de televisión por cable, que limita la propiedad de estaciones de radiodifusión, que dispone que los sistemas satelitales den acceso a programación no comercial

---

34 Cfr. Fiss, O., *The Irony of Free Speech,* Harvard University Press, 1996, Loc. 27 y ss. (versión Kindle).

35 Fiss, *supra* nota 33, Loc. 33. Traducción informal.

o que obliga a los sistemas de cable a transmitir la programación local.[36] Fiss añade a ese grupo –como vimos– la potestad del Estado de usar su chequera para financiar ciertos contenidos.

Estos académicos, entre otros, buscan que esta visión de la libertad de expresión gane terreno en la interpretación de la Primera Enmienda de Estados Unidos. Sin embargo, varias decisiones de la Corte Suprema de Justicia vienen subrayando el contenido individual y autónomo de la libertad de expresión, lo cual condiciona las posibilidades del Estado para intervenir el mercado de ideas. Sin duda, el antecedente reciente más importante es el de *Citizens United v. FEC,* donde la Corte consideró que establecer límites económicos a los gastos de campañas políticas vulnera la libertad de expresión.[37]

Decíamos que el esfuerzo por incorporar esa interpretación democrática o igualitaria de la libertad de expresión es relevante para redefinir los debates sobre derecho de autor. La razón es ésta: justificar la protección de las creaciones intelectuales como una acción positiva del Estado para fomentar y proteger cierto tipo de expresiones pone el mismo derecho en ambos lados de la balanza. Ya no se trata de la tensión entre un derecho aparentemente impermeable a la ponderación y la libertad de expresión, sino de una tensión interna entre libertad de expresión y libertad de expresión.

Desde la perspectiva expresiva, el derecho de autor protege el acceso de autores y audiencias a ciertos tipos de contenidos. O, visto desde el lado contrario, que se pueda copiar fácilmente el trabajo de los autores los hace mucho menos atractivos para quienes los publican o invierten en ellos: ¿para qué pagar por algo que otros pueden obtener gratis?[38]

Tushnet también plantea el argumento en términos de una falla del mercado informativo. En manos de la competencia y el libre flujo de información,

---

36 Cfr. Goodman, E., «Media Policy and Free Speech: The First Amendment at with Itself», en *Free Speech and Copyright Law,* Ed. Audhinarayana Vavili, Amicus Books, The Icfai University Press, 2009, p. 60.

37 Ver Sullivan, K., «Two Concepts of Freedom of Speech», *Harvard Law Review,* 124, 2010, disponible en: http://www.harvardlawreview.org/issues/124/november10/Comment_7328.php (consultada el 6 de diciembre de 2013).

38 Cfr. Tushnet, R., «Copyright as a Model for Free Speech Law: What Copyright Has in Common with Anti-Pornography Laws, Campaign Finance Reform, and Telecommunications Regulation», *Georgetown Law Faculty Publications and Other Works*, Paper Nº 278, 2000, disponible en: http://scholarship.law.georgetown.edu/facpub/278 (consultada el 6 de diciembre de 2013).

ciertos contenidos no serán producidos. Solemos encontrar este fundamento para los medios de servicio público o las obligaciones de información de interés general, pero es igualmente aplicable a los contenidos que por su especialidad, originalidad o costo no serán suministrados por el mercado, o lo serán de manera insuficiente.

«No debe olvidarse que los Redactores pretendían que el copyright fuera en sí mismo un motor de la libertad de expresión. Al establecer el derecho comerciable de usar la expresión de cada uno, el copyright suministra el incentivo económico para crear y diseminar ideas», dijo la Corte Suprema estadounidense en relación con la relevancia del derecho de autor en la Constitución de ese país.[39]

Nos encontramos de nuevo con el argumento económico, pero ya no como base de la propiedad intelectual *per se*, sino como justificación de una intervención estatal que permita fortalecer el debate público. En relación con el bien jurídico que busca preservar el derecho de autor, ya no se trata de garantizar los beneficios económicos del individuo, sino de evitar que disminuya el incentivo del individuo para hablar; de evitar un efecto inhibitorio.[40]

Los valores de libertad de expresión respaldan entonces la acción afirmativa del gobierno de proteger cierto tipo de expresiones privadas.[41] Y esto puede perderse de vista cuando se aboga por la abolición del derecho de autor o se subestima su relevancia. Dejando de lado los argumentos económicos y propietarios, hay también un derecho a la libertad de expresión en ciernes: el de quienes reivindican la potestad de controlar el uso de sus contenidos. El *Centre for Law and Democracy* plantea claramente la disputa de los dos bandos:

> «Quienes proponen la expansión y fortalecimiento del *copyright* –por ejemplo extendiendo el término de protección– alegan que están actuando en el interés de la libertad de expresión al incentivar la creación de contenido nuevo, fortaleciendo de este modo la diversidad de información e ideas disponibles y, a su vez, fortaleciendo los derechos del receptor u oyente. Todo esto mientras también prote-

---

39 Corte Suprema de Justicia de Estados Unidos, *Harper Row v. Nation Enterprises*, 471 US 539 (1985), disponible en: http://www.law.cornell.edu/copyright/cases/471_US_539.htm (consultada el 6 de diciembre de 2013). Traducción informal.

40 Cfr. Tushnet, op. cit., p. 45.

41 Tushnet, op. cit., ps. 37 y ss.

gen los intereses de expresión de los creadores de contenido. Quienes proponen términos más cortos para el *copyright,* por otro lado, reivindican que están promoviendo la libertad de expresión al empujar más material al dominio público, al remover grilletes para la creación de nuevo contenido mediante la reutilización y adaptación, y al permitirles a los consumidores que accedan y compartan el contenido más fácilmente».[42]

Una vez delimitado el conflicto interno entre expectativas válidas pero opuestas de libertad de expresión, es necesario buscar una salida. Y si aceptamos que ambos lados tienen una aspiración legítima en el debate público, la única solución que resulta inaceptable es que uno de ellos ceda del todo a favor del otro. Un sistema que asegure exclusivamente los intereses propietarios de la expresión será tan nocivo como uno que se centre solamente en los terceros que desean usar expresiones de otros individuos. Ahí radica el valor de reubicar el *copyright* en este marco teórico: obliga a hacer un ejercicio de ponderación que desde otros abordajes parece imposible.

Y acá volvemos al rol del Estado como árbitro y distribuidor de oportunidades de expresión. Más allá de que los jueces norteamericanos hayan resistido la visión democrática de la libertad de expresión, es un hecho que existen ejemplos de regulación –en ese país y en otros– donde el Estado ejerce ese rol en la práctica. Cuando el Estado asegura legalmente un derecho de réplica o de rectificación, cuando impone obligaciones de llevar señales y contenidos (*must-carry*) o cuando, como se mencionó, garantiza cuotas mínimas para programas o grupos locales, está abriendo y cerrando, fomentando y limitando, oportunidades de expresión.

Fiss lo compara con el papel que ejerce un parlamentario justo, quien «desea que haya expresiones vigorosas de los puntos de vista, pero también es sensible al exceso de cabildeo y al impacto que tiene en la calidad del debate».[43] Enfrentado ese desequilibrio –agrega Fiss–, el parlamentario le pide al interlocutor que se modere; ha sido tan abusivo en su participación que muchos optaron por abandonar el debate.

Si suponemos que esa moderación que pide un parlamentario a otro es más bien una ley que lo conmina a moderarse, ésta no puede ser desproporciona-

---

42 Centre for Law and Democracy, «Reconceptualising Copyright: Adapting the Rules to Respect Freedom of Expression in the Digital Age», julio 2013, p. 25.

43 Fiss, *supra* nota 33, Loc. 222. Traducción informal.

da y arbitraria. El valor que busca proteger –la libertad de expresión de unos– es a su vez el valor que está en riesgo –la libertad de expresión de otros–. Ese es el ejercicio de ponderación que puede hacer el juez, e incluso el legislador antes de legislar, en *copyright*: ¿esta regulación aumentará la calidad y robustez del debate o tendrá el efecto opuesto?[44]

No hay respuestas automáticas ni fórmulas mágicas. Un ejercicio de ponderación es, en esencia, complejo. Sin embargo, es posible examinar los proyectos de ley y las leyes sobre derecho de autor con estos anteojos. En palabras del juez norteamericano Stephen Breyer, en materia de libertad de expresión, «los jueces deben aplicar presunciones de protección diferentes en contextos diferentes».[45] Una ley que protege los derechos individuales de los creadores no es por naturaleza restrictiva de la libertad de expresión, así como no lo es la ley que promueve un mayor acceso a esas obras.

El enfoque de libertad de expresión no niega los argumentos propietarios y económicos, ni pretende convertirse en un referente autosuficiente para resolver los problemas en torno al derecho de autor. Debe ser útil, más bien, para poner esos argumentos en perspectiva, para darles contenido y algún nivel de compatibilidad de lado y lado que permita llevar a cabo el ejercicio de balance del que venimos hablando.

A manera de ilustración –y ya para terminar– hagamos un ejercicio inicial de ponderación en el caso de las excepciones al derecho de autor. En el sistema norteamericano, el «uso justo» o *fair use* permite usar contenidos protegidos sin autorización del titular para hacer comentarios, críticas o parodias. Sin embargo, la práctica de hacer remezclas o *mashups* en el entorno digital –combinar porciones de videos o audios, o tomarlas para crear un nuevo producto– puede desbordar fácilmente la protección de uso justo si, por ejemplo, incluye fragmentos muy largos del material original.

¿Esta restricción tiene la virtud de proteger los intereses expresivos de los creadores? ¿De qué manera afecta el interés colectivo de tener más expresiones en el debate público? Estas preguntas en sí mismas pueden orientar la ponderación y, a su vez, complementar el análisis tradicional del incentivo econó-

---

[44] Cfr. Fiss, *supra* nota 33, Loc. 187.

[45] Breyer, disidencia, en Gil Garcetti *et al., Petitioners vs. Richard Ceballos,* mayo de 2006, disponible en: http://www.washingtonpost.com/wp-srv/nation/supremecourt/Garcetti_Ceballos.htm (consultada el 6 de diciembre de 2013). Traducción informal.

mico que, como vimos, no es fácil de asir. A partir de esto, una ponderación interna de intereses expresivos podría indicar que el «uso justo» debería permitir la práctica de remezclas y *mashups*.

En estos mismos términos, el ejercicio de ponderación podría aplicarse –tanto en la instancia del diseño de la regulación como en la de revisión judicial– a las demás áreas donde el *copyright* viene expandiéndose: las Medidas Tecnológicas de Protección, que estrechan demasiado el uso externo de contenido protegido; la extensión de los términos de protección, y los mecanismos de notificación y retiro –como el del *Digital Millennium Copyright Act*– que permiten controlar contenidos sin que medie algún tipo de control judicial.[46]

En el contexto latinoamericano, esta propuesta de repensar el pulso entre el derecho de autor y la libertad de expresión como una tensión interna, resulta especialmente importante: a diferencia del sistema norteamericano, donde la cláusula de «uso justo» es un tanto flexible y se presta a interpretación, la mayoría de regímenes de nuestra región –siguiendo tratados internacionales– establecen que las excepciones al uso de material protegido son taxativas y específicas. Tal abordaje, de entrada, da prelación a los intereses expresivos de los autores por encima de los de los demás ciudadanos. Habría que comenzar por preguntarse, entonces, si en estos sistemas el Estado está distribuyendo las oportunidades expresivas de manera democrática. Y la respuesta ya no puede ser, escuetamente, que la propiedad del derecho de autor y su conveniencia económica lo justifican.

III. Recomendaciones

• Los argumentos propietarios y económicos aíslan el *copyright,* como una especie de derecho autónomo y autosuficiente. Desde allí es difícil cuestionar el impacto que tiene esta regulación en la libertad de expresión.

• Delimitar el conflicto entre *copyright* y libertad de expresión como una tensión interna entre dos expectativas válidas de expresión, puede dar luces para hacer una mejor ponderación de los intereses involucrados.

• Si se acepta que ambos lados tienen una aspiración legítima en el debate público, resulta inaceptable cualquier solución que implique que uno de ellos ceda del todo a favor del otro.

---

46 Cfr. Cortés Castillo, *supra* nota 30.

• A pesar del reto que implica un ejercicio de ponderación, es posible examinar los proyectos de ley y las leyes sobre derecho de autor de esta perspectiva. Y es necesario hacerlo sin tener una visión predefinida de cuál es la protección más importante.

• El enfoque de libertad de expresión puede dar luces para revisar normas de notificación y retiro, extensiones de términos de protección del derecho de autor, y el uso extendido de Medidas Tecnológicas de Protección.

Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital[1]

Resumen

Este documento analiza el debate sobre el derecho al olvido en Internet, que viene desarrollándose en algunos países y proponiéndose formalmente en Europa. El documento está dividido en las siguientes partes: i) la abundancia de información en Internet; ii) el efecto multiplicador de la agregación y la indexación de datos; iii) la relación entre la abundancia de datos y el control; iv) el problema de recordar en la era digital; v) algunas definiciones propuestas para el derecho al olvido; vi) el debate entre este derecho como una solución o un problema, y vii) algunas propuestas prácticas para introducir una especie de olvido en el entorno digital. Al final, se hacen las siguientes recomendaciones:

• El marco normativo de la protección de datos es un punto de partida para desarrollar la discusión, pero no parece suficiente en el contexto de un entorno digital donde la información tiene formas y modalidades heterogéneas, se origina en múltiples fuentes y trasciende los criterios tradicionales del manejo de bases de datos.

• La discusión jurídica no puede darse sin tomar en cuenta las fuerzas que moldean e interactúan en el desarrollo de Internet. El mercado, la interacción

[1] Este documento fue elaborado por Carlos Cortés Castillo, investigador de la Iniciativa por la Libertad de Expresión en Internet (iLEI), del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo. La investigación y elaboración del documento fue dirigida y contó con los comentarios de Eduardo Bertoni, director del CELE.

social y el código –en el sentido informático– son variables interdependientes que definen y habilitan el entorno digital.

• Las propuestas técnicas para introducir un olvido no deben pasar desapercibidas. Ya sea a través de mecanismos legales o de autorregulación, ideas como éstas podrían servir para abordar la propuesta de una especie de derecho al olvido que preserve el equilibrio de los derechos humanos involucrados.

• Se debe tener en cuenta la tensión en materia de protección de datos y privacidad entre la aproximación europea y la norteamericana. Resulta importante tener en mente este antecedente para observar la manera en que esos casos se analizarían a la luz de la Convención Interamericana de Derechos Humanos.

• El análisis del caso del derecho al olvido sugiere que una primera respuesta es buscar que sean los intermediarios quienes resuelvan los problemas, so pena de ser responsables. Sin embargo, se deben buscar soluciones que abarquen un contexto más amplio; que además de los intermediarios tomen en cuenta a los demás actores involucrados en Internet, empezando por los propios usuarios.

I. Introducción

En su libro *Borrar: la virtud de olvidar en la era digital*, Viktor Mayer-Schönberger plantea una idea fundamental sobre el cambio de paradigma en la memoria como consecuencia del desarrollo tecnológico: en la época del libro y la tradición oral, olvidar era la regla general y recordar, la excepción; pero en tiempos de grabaciones y archivos digitales y bases de datos en línea, recordar es la norma. Sólo se olvida lo que se deshecha de manera explícita.[2]

Mayer-Schönberger no atribuye ese cambio a un desarrollo del cerebro humano, cuya capacidad fisiológica es, en términos generales, la misma desde hace 100 años. La habilidad de recordar se debe al apoyo de la tecnología –desde la imprenta hasta las computadoras–, que de manera paulatina viene incrementando las posibilidades de registro y almacenamiento de toda actividad humana. Según el autor, la imposibilidad de olvidar nos pondrá en el futuro en los zapatos de Ireneo Funes, el personaje del cuento de Jorge Luis Bor-

---

[2] Véase Mayer-Schönberger, Viktor, *Delete: The Virtue of Forgetting in the Digital Age,* Princeton, Princeton University Press, 2009.

ges que recordaba las veces que había imaginado o visto «cada hoja de cada árbol de cada monte».

Hoy por hoy, Internet media casi todas las actividades cotidianas de las personas. El consumo de noticias, las relaciones laborales y personales, los momentos de esparcimiento y los temas financieros y de salud suelen involucrar el uso de aplicaciones móviles, servicios en línea y toda clase de intermediarios.

Este cambio no solo tiene consecuencias en la manera como las personas afrontan su presente y referencian su pasado, sino también en el tipo de relación que tienen con su información personal y en las dinámicas que genera el movimiento de datos personales en la red. Más precisamente, este cambio implica una redefinición del control de la información sobre nosotros mismos, la cual nos identifica y a la vez nos permite definirnos.

En este contexto se viene dando un debate sobre la necesidad de crear un derecho al olvido que, por una parte, le devuelva al individuo el control sobre su información y, por otra, le permita liberar su pasado de un rígido molde digital. Así, el derecho al olvido busca, por ejemplo, que una empresa no tenga más en su poder cierto dato sobre alguien, que mis amigos dejen de ver en las redes sociales la foto de mi excursión de bachillerato de hace diez años, o que un motor de búsqueda excluya de sus resultados los rumores falsos que acabaron con la reputación de alguien.

Los críticos de esta idea también apuntan a ejemplos en que parece menos conveniente hablar de olvido: un político corrupto que desea que no se hable más de su oscuro pasado, un policía buscando que se elimine un video donde acepta un soborno, un médico tratando de eliminar un registro sobre una mala práctica profesional.

El propósito de este documento es, entonces, presentar y explorar este debate. Aunque la idea del derecho al olvido no es nueva, viene avanzando con más fuerza desde enero pasado, cuando la Comisión Europea presentó una propuesta para reformar la normativa sobre protección de datos. Y es ahí donde arranca el debate: ¿es lo mismo hablar de derecho al olvido que de protección de datos?, ¿es realmente algo nuevo?

El documento está dividido en las siguiente partes: primero, la abundancia de información en Internet; segundo, el efecto multiplicador de la agregación y la indexación de datos; tercero, la relación entre la abundancia de datos y el control; cuarto, el problema de recordar en la era digital; quinto, algunas definiciones propuestas para el derecho al olvido; sexto, el debate entre este derecho como una solución o un problema, y séptimo, algunas propuestas prácticas para

introducir una especie olvido en el entorno digital. Por último, ofrecemos algunas conclusiones y recomendaciones.

Es importante aclarar que este documento busca ofrecer un panorama general del tema antes que un análisis pormenorizado de los elementos jurídicos, regulatorios y técnicos. Y aunque señalamos razones por las que la discusión sobre el derecho al olvido es importante, no pretendemos asumir la defensa de su implementación. Consideramos que, sobre todo, resulta importante entender los argumentos en juego, ubicar –especialmente– las distintas posiciones y empezar a pensar el tema desde América Latina.

II. Nuestra vida, volcada a la red

No hay que ser un usuario de Internet de tiempo completo o un adicto a las redes sociales para que decenas de datos sobre uno estén alojados en diferentes puntos de la red. Tomemos como ejemplo el correo electrónico: con un servicio como Gmail, una persona puede tener archivados todos los mensajes que ha enviado y recibido desde 2004, incluidos los que intercambió a través del servicio de chat. A lo anterior podemos sumar la información almacenada en Facebook. Fotos, videos, conversaciones, archivos y, en general, cualquier intercambio que haya dejado un rastro digital desde el momento en que se abrió la cuenta.

Incluso si esa persona prescindió de esos servicios o los uso mínimamente, otra actividad habitual en línea –cuyo efecto es tal vez menos visible– deja un rastro abundante: las búsquedas hechas en motores de búsqueda como Google, Yahoo! o Ask. Con algunas diferencias propias de la política de cada empresa, los términos que se introducen en estos servicios se guardan en un servidor y conforman un historial. Entre otros, esta información sirve para ajustar la publicidad que aparece en las páginas que la usuaria visita y para moldear los propios resultados de las búsquedas.

Aunque algo de esta información se almacene de manera anónima, la sumatoria de datos permite perfilar con bastante precisión a una persona. Si a la dirección IP de un computador –que identifica su conexión en Internet– se van sumando variables como búsquedas de lugares (direcciones de hoteles, casas o restaurantes), medicinas, entradas de eventos, ropa o comida, al final será posible determinar de quién se trata.

Sin embargo, no es usual hacer indagaciones ordenadas o coherentes en los motores de búsqueda. En un momento dado alguien puede buscar todo lo referente a un tema laboral y, un segundo después, hacer una consulta sobre un problema de salud o una idea descabellada o pasajera (le surge la

curiosidad, por ejemplo, de averiguar sobre una persona con la que tuvo una relación sentimental hace muchos años). En estos casos, los datos que se van registrando no solo perfilan a una persona de manera equivocada o descontextualizada, sino que se refieren a temas que ésta quisiera mantener en su órbita privada.

Más allá de este problema, resulta claro que la agregación, indexación y etiquetación de datos sobre un persona tienen un efecto multiplicador. Un conjunto de datos sobre la actividad de una persona en Internet no equivale simplemente a una suma de informaciones aisladas. A medida que agregamos más información tendremos una radiografía más precisa de algún aspecto del individuo.

Aquí no podemos limitarnos únicamente a la información que el usuario de Internet suministra sobre sí mismo y que termina en poder de un tercero (en el servidor de Amazon o de Twitter). Diferentes datos sobre nosotros mismos pueden estar en línea después de que un tercero los hizo disponibles, aun sin nuestro consentimiento o conocimiento: alguien colgó y etiquetó una foto suya en Facebook sin que usted lo supiera; una entidad oficial publicó en el portal una base de datos que contiene su nombre; un medio de comunicación publicó una historia donde incluye información sobre usted; un usuario anónimo creó un blog para criticarlo, incluyendo de pronto información sobre su vida privada.

También es posible que la información en línea sobre una persona esté ahí porque ella misma la publicó y, aunque posteriormente la retiró, alguien más hizo una copia y la mantuvo disponible en otro lugar. No hay que limitar este caso a un robo o un acto de mala fe: piense, por ejemplo, que hace tres o cuatro años usted publicó de manera entusiasta en Facebook unas fotos de su fiesta de cumpleaños. Ahora las ve y las elimina –le parecen pasadas de moda, ya no le evocan un momento alegre o simplemente no le gustan más–. No obstante, un amigo las copió mucho antes y las tiene colgadas en su blog personal. Por más que usted no quiera, cualquier persona podrá seguir accediendo a esa información.

II.A. El efecto multiplicador de la agregación y la indexación

En resumen, los datos que se pueden encontrar en Internet sobre una persona, tanto los que la identifican como los que se refieren a ella de algún modo, tienen dos fuentes generales: la propia persona o un tercero. Y a medida que se copian o se re-publican (*reposting*) siguen diferentes caminos. Para entender mejor el problema del efecto multiplicador de los datos, el consiguiente riesgo de descontextualización y el impacto en la órbita privada,

tomemos un ejemplo más detallado y supongamos los siguientes cuatro hechos aislados:

a) Ramiro utiliza Foursquare, una aplicación que permite notificar a los contactos acerca del sitio donde uno se encuentra. A las diez de la mañana del jueves, Ramiro ingresa a un café aledaño a un hospital de la ciudad y se registra en Foursquare desde su teléfono móvil. Una notificación con esa información le llega a sus contactos.

b) Con cada vez más frecuencia, las discotecas toman fotografías durante sus fiestas y las cuelgan en sus sitios de Internet. Este jueves no es la excepción en «El Boliche». Las fotos de la noche anterior ya están disponibles. Un amigo de Ramiro ingresa al sitio y ve una foto de aquél en medio de la fiesta. Aunque no estuvo con Ramiro esa noche, la foto le parece divertida y la etiqueta.

c) Ramiro también es usuario de Twitter, el popular servicio de microblogs y mensajes. Durante la tarde del miércoles intercambió algunos mensajes agresivos con un ex compañero de trabajo. La cosa no pasó de unos insultos por un tema aparentemente sin importancia.

d) Hacia el mediodía, un medio de comunicación local reporta que el miércoles en la noche hubo una pelea en «El Boliche» y tuvo que intervenir la Policía. Según las autoridades, al parecer, la pelea fue entre dos jóvenes que habían estado enviándose mensajes por Internet desde la tarde.

Ramiro puede ser cualquier joven de 20 años con una vida activa en Internet y con cuentas abiertas en varias redes sociales. Si nos enteramos de cualquiera de estos hechos de manera independiente, no tendremos ningún dato relevante sobre él: entró a una cafetería, estuvo en una fiesta el miércoles en la noche, tuvo un altercado en Twitter, hubo una pelea en «El Boliche». Pero si tenemos acceso a todos los datos sobre él –ya sea porque alguien los agregó en un sitio o porque hicimos una búsqueda por el nombre, en cuyo caso aparecen indexados– podemos inmediatamente especular: Ramiro estuvo en el hospital después de estar en la fiesta de «El Boliche»; estuvo involucrado en una pelea con una persona por una discusión previa a través de una red social; tal vez salió herido.

Este relato puede tener un impacto entre los amigos de Ramiro y tomarse como cierto más allá de que la verdad sea distinta. En la medida en que la agregación e indexación de datos se refieran al buen nombre o la vida privada de alguien, el choque con la veracidad de la información se hará más palpable.

Tomemos el caso de un medio de comunicación que acusa a un político por corrupción. Supongamos que posteriormente se comprueba que la informa-

ción es falsa o poco veraz, y aunque el medio rectifica en su versión impresa, la versión digital continúa accesible al público y ha sido republicada por otros portales en línea. Y supongamos también que a esta información se suman afirmaciones del involucrado sacadas de contexto y otros datos provenientes de distintas fuentes que resultan igualmente falsos o incompletos (supongamos que alguien juntó todo eso en un sitio de agregación de redes sociales). «La distinción antigua entre la circulación de hechos y la diseminación de opiniones ha sido borrada de tal manera que ambas se están graduando en el mismo tipo de visibilidad», dice el antropólogo y filósofo francés Bruno Latour.[3] Una simple búsqueda en Internet bastará para encontrar hechos, opiniones y especulaciones en un solo lugar y con el mismo rango aparente de importancia.

La agregación de datos resulta aún más poderosa con los motores de búsqueda que funcionan con algoritmos. Cuando el usuario comienza a teclear un término, rápidamente el programa le ofrece autocompletar la búsqueda. Si uno escribe «Barack», inmediatamente aparecerá «Obama». La sugerencia es el resultado de cruzar variables como búsquedas comunes en la red o disponibilidad de información. Sin embargo, lo que es aparentemente una función cómoda y expedita puede aparejar una distorsión de la realidad.

El caso más conocido en Europa es el de la ex primera dama de Alemania Bettina Wulff, quien demandó a Google por la función de autocompletar asociada a ella: cuando alguien tecleaba su nombre, el motor de búsqueda sugería términos como «dama de compañía» (*escort*) o «prostituta», un rumor sobre ella que se mueve en la red sin que haya, hasta ahora, algún sustento veraz.[4] Con la acción judicial, Wulff básicamente pretende que Google se «olvide» de una información sobre ella. Aunque es imposible que esa asociación se borre de todos los blogs o foros difamatorios que abundan en Internet, empezarán a ser invisibles si el algoritmo los ignora.

Algo similar sucedió en Argentina con la cantante y modelo Virginia Da Cunha, cuyo nombre en los resultados de los motores de búsqueda aparecía

---

3 Latour, Bruno, «Beware, your imagination leaves digital traces», *Times Higher Literary Supplement,* 6 de abril de 2007. Traducción informal.

4 Véase Lardinois, Frederic, «Germany's Former First Lady Sues Google For Defamation Over Autocomplete Suggestions», *Techcrunch,* 7 de septiembre de 2012, disponible en: http://techcrunch.com/2012/09/07/germanys-former-first-lady-sues-google-for-defa mation-over-autocomplete-suggestions/ (consultada en noviembre de 2012).

asociado a sitios de pornografía. Al parecer, varios de estos sitios albergaban fotomontajes pornográficos de ella. En 2009, Google y Yahoo! fueron condenados en primera instancia a pagar una indemnización a Da Cuhna. Posteriormente, en segunda instancia, fueron exonerados bajo un análisis de exención de responsabilidad de los intermediarios.[5]

Estos ejemplos sirven para ilustrar dos puntos; por un lado, la agregación e indexación de información tiene un efecto poderoso en términos de lo que se puede decir –o aparentar decir– sobre una persona. Mientras en el mundo análogo la difusión de pedazos de información erróneos, inexactos o indeseados tiene un alcance limitado, en el mundo digital el impacto es inagotable y los efectos pueden ser perversos. Por el otro, esta información es pública y llega a la red por varios caminos. Esto implica que tratar de contrarrestarla o disponer de ella (borrarla, modificarla) no depende únicamente del afectado ni pasa por la responsabilidad exclusiva de un intermediario. Que Internet se «olvide» de esos datos requiere algo más que oprimir una tecla.

III. Más datos, menos control

Entre más «digitalizamos» nuestras vidas, menor es el control que tenemos sobre nuestra información. Nuestras conversaciones íntimas están en el correo electrónico o en el servicio de chat; nuestras fotos, en un casillero en línea; nuestros datos bancarios, en la última tienda en línea donde compramos algo; cualquier dato sobre nuestro estado de salud, en una base de datos en un hospital o en el historial de compras de la farmacia.

La facilidad técnica para copiar y almacenar información, los decrecientes costos de las computadoras y los dispositivos móviles, y el aumento en la capacidad de aparatos y aplicaciones para procesar datos, constituyen incentivos para que las personas tiendan a acumular datos sobre sí mismas y sobre otras. Cuando debíamos revelar rollos para obtener fotografías, escogíamos los momentos para tomar una foto o seleccionábamos solo las mejores imágenes de los negativos. El proceso era costoso tanto en tiempo como en dinero. Más adelante, con la computadora personal, nos preocupábamos de no llenar el disco duro de archivos innecesarios, así como borrábamos correos electró-

---

[5] Véase Braginski, Ricardo, «Google y Yahoo! dan vuelta un fallo contra una ex Bandana», *Clarín,* 16 de agosto de 2010, disponible en: http://www.clarin.com/internet/Google-Yahoo-vuelta-fallo-Bandana_0_317968397.html (consultada en noviembre de 2012).

nicos para no copar la capacidad de nuestro buzón. Hoy nada de eso es necesario: tomamos decenas de fotos, guardamos todo los archivos y mensajes. Ahora lo costoso es tomarse el tiempo de seleccionar y descartar.[6]

Desde el punto de vista comercial, el incentivo para acumular datos es innegable. Si una librería en línea sabe qué libros compró una persona en el último año, podrá ofrecerle solamente los géneros literarios que le interesan; si un supermercado puede guardar el historial de compras de una familia, podrá ofrecerle paquetes mensuales con descuentos y productos similares. Para el negocio de la publicidad, cuyo objetivo último es lograr que la atención de un comprador termine en una compra, la acumulación de datos equivale a una mina de oro. Nir Eyal lo llama el proceso de «manufacturar el deseo», donde nada importa más que saber de antemano qué quiere el consumidor.[7]

Si bien los agentes que captan información de los usuarios la manejan y centralizan, es equivocado pensar que adquieran un control absoluto sobre ésta. Por un lado, la creación de una base de datos, o simplemente de un lugar donde haya información alojada, contiene riesgos implícitos en términos de seguridad. «En últimas, donde quiera que haya datos, hay vulnerabilidad; de manera que la única forma en que los datos no son vulnerables es que no existan», afirma Paul Bernal.[8] Cualquier sistema de información debe tener al menos una puerta de entrada, y por más sofisticada que sea su seguridad siempre dependerá –o debe depender– de la interacción humana. Por el otro lado, las bases de datos son en sí mismas una mercancía que se mueve en todos los mercados.

Entre más funcional y desarrollada es una base de datos, mayor es su potencial. Por ejemplo, una tabla de Excel sobre gastos de campañas electorales ordenada por categorías, nombres y fechas es infinitamente más útil que un documento impreso, sin uniformidad y con errores tipográficos. En términos de transparencia y acceso a la información se espera que las autoridades reporten este tipo de información en un formato que pueda procesarse. Pero

---

6 Véase Mayer-Schönberger, *supra* nota 2.

7 Véase Eyal, Nir, «How To Manufacture Desire», *Techcrunch,* 4 de marzo de 2012, disponible en: http://www.techcrunch.com/2012/03/04/how-to-manufacture-desire/ (consultada en noviembre de 2012).

8 Bernal, Paul, «A Right to Delete?», *European Journal of Law and Technology*, Vol. 2, Nº 2, 2011, disponible en: http://ejlt.org/article/view/75/144, p. 6. Traducción informal.

esta utilidad puede ser un problema si en vez de una campaña electoral se trata de la historia clínica de un grupo de pacientes psiquiátricos. Usando herramientas adecuadas de consulta y cruce de referencias podemos obtener información que, sin duda, hace parte de la esfera privada de esos individuos. Si a esto sumamos los puntos de entrada que puede tener un sistema de información –piénsese, por ejemplo, en todas las terminales de consulta de un hospital– podemos entender que en un universo digitalizado la información también es sinónimo de riesgo.

El control es entonces apenas una cara de la moneda en cuyo lado opuesto está la dispersión y la descentralización. Nuestra información no está en manos de nadie y a la vez puede estar en manos de muchos. Sumado a los incentivos para acumular datos y los costos de borrarlo, nos enfrentamos a un entorno de información creciente que no podemos asir. «Podemos llegar a sufrir una reducción en el control de nuestra información antes de darnos cuenta. Del mismo modo, otros ganan en poder informacional a partir de nuestra pérdida, influenciando las circunstancias de nuestras interacciones futuras con el mundo», apunta Mayer-Schönberger.[9]

IV. El problema de recordar

La buena memoria suele verse como una virtud antes que un defecto. En el caso de las instituciones, la preservación de la historia no solo es un deber sino también una condición necesaria de eficiencia. Sin embargo, para Mayer-Schönberger el cambio de paradigma de la memoria –de olvidar como regla general a olvidar como excepción– afecta la manera como el individuo interpreta su pasado y vive su presente. En esencia, olvidar le permite al hombre desarrollar sus convicciones y creencias y ajustarlas al presente; le posibilita cambiar, reinterpretar, innovar e incluso perdonar.

El autor plantea una situación cotidiana: una persona va reencontrarse con un amigo al que no ve hace muchos años y que está de visita en la ciudad. Emocionada por volver a verlo, intercambia correos con él para concertar una cita. Y mientras busca el último mensaje para contestarle, se encuentra con una serie de correos electrónicos de hace varios años donde tuvo una pelea con él por cualquier motivo. Ya había olvidado ese episodio. Ahora lo revive y reinterpreta su presente.[10]

---

9 Mayer-Schönberger, *supra* nota 2, pos. 1160 (versión Kindle).

10 *Ibídem.*

Con ocasión del aniversario 25 del asesinato de su padre, el escritor colombiano Héctor Abad Faciolince escribió una entrada en su blog titulada «Acuérdate de olvidar», donde se declara cansado de recordar un episodio tan doloroso durante tanto tiempo:

> «Yo reconozco la importancia política de tener una memoria larga. Eso hace que los asesinos no se sientan nunca a salvo: su crimen será recordado. Tal vez por nuestra memoria a ellos les tiemble la mano cuando piensen otra vez en apretar el gatillo. Sí, es importante recordar. Pero hay también una necesidad privada de olvidar, o mejor, de recordar otras cosas».[11]

Se trata, por supuesto, de dos ejemplos radicalmente diferentes. Sin embargo, guardan en común el reto de adaptarse al pasado y vivir el presente en medio de una penetrante memoria digital. Hace 20 años, dos amigos no tendrían documentadas sus peleas en mensajes. Aquellos desencuentros estarían desteñidos por la memoria y recontextualizados en el presente. Y hace 20 años, el recuerdo de un familiar fallecido no estaría mediado por tal cantidad de videos, fotos, audios y perfiles en redes sociales –una «vida» digital que no perece–.

Abad Faciolince plantea la idea del olvido también como la posibilidad de recordar algo diferente y no siempre lo mismo. En su caso se trata del trágico día en que asesinaron a su padre. Pero la afirmación resulta igualmente útil a la luz de la memoria en la era digital. A pesar de que, como decíamos, la actividad humana está cada vez más documentada en la red, largas porciones de ésta quedan fuera de ese registro: conversaciones personales, encuentros, movimientos, actividades cotidianas y, sobre todo, las interpretaciones y sensaciones del individuo. Pero a medida que pasa el tiempo la memoria digital nos ofrece siempre el mismo recuerdo: el mismo video o el mismo intercambio de mensajes. Nuestra memoria se condiciona entonces a los episodios registrados y deja de lado los demás. Tomamos como referente del pasado un recuerdo objetivizado en detrimento del subjetivo y personal.

Ese pasado estático –argumentan algunos autores– se vuelve un obstáculo para el desarrollo personal. Teniendo un referente tan aparentemente claro de

---

[11] Abad Faciolince, Héctor, «Acuérdate de olvidar», *El Espectador*, 25 de agosto de 2012, disponible en: http://blogs.elespectador.com/habad/2012/08/25/acuerdate-de-olvidar/ (consultada en noviembre de 2012).

lo que hizo o pensó en el pasado, el individuo no se permite olvidar o cambiar. Según Liam Bannon, «olvidar no es una desafortunada limitación del ser humano, sino más bien una actividad mental necesaria que nos ayuda a filtrar la inundación sensorial entrante, y así nos permite actuar en el mundo».[12] A pesar de que las acciones anteriores se examinan desde un presente totalmente distinto en tiempo, modo y lugar, se convierten en un molde rígido para actuar. En consecuencia, el individuo se vuelve proclive a la autocensura e inhibición.[13]

El contra-argumento más importante frente al problema de recordar se refiere a la «adaptación cognitiva», que no es otra cosa que la capacidad del ser humano de asimilar cambios. «La gente, especialmente la gente más joven, ideará mecanismos de supervivencia. Ese va ser el cambio, no una intervención de cualquier cuerpo gubernamental o tecnológico», responde Danah Boyd.[14] Al final de cuentas –siguiendo ese planteamiento–, el ser humano logrará ajustar su proceso cognitivo para evitar que el pasado, documentado y al alcance de la mano, nuble su juicio.

Una idea similar, que también se relaciona con una de las soluciones propuestas por algunos autores, apunta al beneficio de una «sobredosis» de información. A medida que la memoria digital avanza y se profundiza, la persona logrará poner en contexto su pasado sin temor a perder la perspectiva.

De una u otra forma, en el mundo digital ya se ven algunos síntomas del impacto negativo que tiene ese pasado objetivado y anecdótico, representado en un dato cualquiera, como una imagen o un texto sobre el cual el titular ya no tiene control. En septiembre pasado, Amanda Todd, una canadiense de 15 años, publicó un video en Youtube donde decía que había sido víctima de

---

[12] Bannon, Liam J., «Forgetting as a feature, not a bug: the duality of memory and implications for ubiquitous computing», *CoDesign,* Vol. 2, Nº 1, marzo de 2006, ps. 3-15. Traducción informal.

[13] Véase Mayer-Schönberger, *supra* nota 2, pos. 1701 y ss.

[14] Winter, Jessica, «The advantages of amnesia», *The Boston Globe,* 23 de septiembre de 2007, disponible en: http://www.boston.com/news/education/higher/articles/2007/09/23/the_advantages_of_amnesia/?page=full (citando a Boyd, Danah) (consultada en noviembre de 2012). Traducción informal.

ciberacoso. A través de un chat había compartido una foto íntima de ella con un hombre que posteriormente la quiso ridiculizar con el material y lo difundió entre sus amigos y conocidos. Unas semanas después, Todd se suicidó.[15]

Aunque para algunos este episodio hace parte del fenómeno conocido del matoneo o acoso entre jóvenes y adolescentes, parece claro que en el contexto de Internet tiene la propensión de escalar (conocido como *cyberbullying*). «Un derecho al olvido podría ofrecer una esperanza para las víctimas de “cyberbullying”», plantea Ambrose tomando el caso de Todd como antecedente.[16] Ese ejemplo es uno más de una lista que crece diariamente. Un episodio reciente y apenas anecdótico, que en otra época sería dejado atrás rápidamente, puede perseguir a un individuo de manera incesante. Lo cual parece más complejo frente a generaciones que nacieron y crecieron en la era digital.

V. En busca de una definición

La necesidad de un «derecho al olvido» se ha planteado en el contexto esbozado anteriormente. Aunque el problema que se busca abordar parece claro, el significado y contenido de la solución es, por ahora, borroso. En esta parte del documento esbozaremos una definición de derecho al olvido y lo relacionaremos con el derecho a la protección de datos o hábeas data. En el centro de esta discusión están los interrogantes de si es posible elaborar un derecho al olvido a partir de las garantías existentes y si, de llegar a instituirlo, chocaría con otros derechos.

Paul Bernal ubica el origen del derecho al olvido en el concepto legal francés del *droit à l'oubli* y el italiano *diritto all'oblio*, que en términos generales se entienden como «el derecho a silenciar eventos pasados de la vida que ya no están sucediendo».[17] Meg Ambrose concuerda, y afirma que el término francés incluye tanto el derecho a ser olvidado como la obligación de olvidar.

---

[15] Véase Ambrose, Meg Leta, «Bullying and the Right to be Forgotten: A Right to End Victimization», en: *www.playgiarizing.com,* 12 de octubre de 2012, disponible en: http://playgiarizing.com/2012/10/12/bullying-and-the-right-to-be-forgotten-a-right-to-end-victimization/ (consultadaa en noviembre de 2012).

[16] *Ibídem.*

[17] Bernal, *supra* nota 8 (citando a Pino, G., «The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights», en Hoecke M. V. y Ost (eds.), *The Harmonisation of European Private Law,* Bruselas, Hart, 2000, p. 237.

Esta distinción es importante, toda vez que el enfoque de esta garantía determina en cabeza de quién están las prestaciones para hacerla cumplir.[18]

Siguiendo de alguna manera el enfoque de Mayer-Schönberger sobre la necesidad humana de olvidar, la Comisión Nacional de Informática y Libertades de Francia –el ente autónomo que protege el procesamiento de datos en ese país– considera que el derecho al olvido (o a ser olvidado) es el derecho a cambiar, evolucionar y contradecirse. La Comisión lo concretiza en el «Principio de duración limitada de la retención de datos», según el cual la información no puede conservarse en ficheros digitales indefinidamente, sino únicamente por el tiempo necesario para cumplir con el propósito para el cual fue recogida.[19]

V.A. Del hábeas data al olvido

Esta conceptualización del derecho al olvido se erige sobre instituciones jurídicas conocidas. Desde tiempo atrás, la mayoría de legislaciones en el mundo contemplan la prescripción de delitos, el borrado de antecedente penales o las amnistías en temas tributarios y financieros. En muchos de estos casos, se utiliza explícitamente el término «derecho al olvido». En Argentina, por ejemplo, la ley 25.326 dispone que el término de archivo de los antecedentes crediticios de una persona es de cinco años, plazo que se reduce a dos cuando los deudores –en caso de acreencias– paguen su obligación.

Las normas sobre protección de datos –o hábeas data– se han desarrollado en distintos países de la región principalmente a través de leyes. En el reciente fallo que revisó la constitucionalidad de la ley estatutaria de hábeas data de Colombia, la Corte Constitucional de ese país enumeró los contenidos mínimos de este derecho:

> «(i) el derecho de las personas a conocer –acceso– la información que sobre ellas está recogida en bases de datos (…); (ii) el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; (iii) el derecho a actualizar

---

18 Véase Ambrose, Meg Leta, «You Are What Google Says You Are: The Right to be Forgotten and Information Stewardship», *International Review of Information Ethics,* Vol. 17, 2012, disponible en: http://ssrn.com/abstract=2154353.

19 Véase Commission Nationale de L'Informatique et Des Libertés, «Rapport d'activité 2011», disponible en: http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/RA2011_CNIL_FR.pdf.

> la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida (…); (v) el derecho a excluir información de una base de datos».[20]

La Agencia Española de Protección de Datos, de hecho, ha abordado el derecho al olvido desde esa órbita, propia de su competencia (a esto volveremos más adelante). En un sentido similar, en enero de 2012, la Comisión Europea dio a conocer una propuesta para reformar la Directiva de Protección de Datos adoptada por la Unión Europea en 1995. Entre otros temas, ésta contempla la introducción formal del derecho al olvido:

> «(…) a los interesados les debe asistir el derecho a que se supriman y no se traten sus datos personales, en caso de que ya no sean necesarios para los fines para los que fueron recogidos o tratados de otro modo, de que los interesados hayan retirado su consentimiento para el tratamiento, de que se opongan al tratamiento de datos personales que les conciernan o de que el tratamiento de sus datos personales no se ajuste de otro modo a lo dispuesto en el presente Reglamento».[21]

La propuesta, que marcó simbólicamente el inicio del debate sobre este tema, incluye también la posibilidad de que el usuario revoque el consentimiento sobre el uso de la información que hubiera dado cuando era menor de edad, «cuando no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quisieran suprimir tales datos personales especialmente en Internet».[22]

Tal obligación de supresión impone deberes a los responsables del tratamiento de datos, es decir, a quien los capta y administra, como Twitter o Facebook. En teoría, además de tener que borrar eventualmente un dato, una empresa como Facebook tendría que asegurarse de que los terceros que accedieron a esa información por cuenta de la difusión que hizo aquélla, sepan que el interesado está solicitando la supresión de esos datos personales. Y si el ter-

---

20 Corte Constitucional de Colombia, sentencia C-748-11. Magistrado ponente: Jorge Ignacio Pretelt.

21 Comisión Europea, «Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos», Bruselas, 25 de enero de 2012, COM(2012) 11 final, párrafos 53 y ss.

22 *Ibídem.*

cero accedió con autorización de Facebook, este último es responsable de la publicación hecha por ese tercero.

Igualmente, la Comisión Europea busca fortalecer la garantía de portabilidad de los datos (en esencia, que el usuario pueda «llevarse» sus datos cuando abandone un servicio) y que se desarrollen medidas para evitar la elaboración de perfiles automáticos que no fueron consentidos por la persona (conocido como *profiling*). Es decir, esta disposición busca evitar el problema de agregación de datos sobre una persona que –como se explicó al comienzo de este documento– puede resultar en una descripción distorsionada y deshumanizada del individuo.

En busca de un equilibrio, la propuesta europea estipula una serie de excepciones: se podrán conservar datos con fines históricos y científicos por razones de interés público, como la salud pública, la libertad de expresión y por otro motivo que amerite su preservación en cumplimiento de una ley particular. Y es ahí donde está el nudo del derecho al olvido. Por un lado, algunos consideran que por vía de excepciones puede volverse efímero y, por el otro, algunos argumentan que su aplicación podría terminar por sofocar otros derechos igualmente importantes y contribuir al desmonte del Internet abierto que conocemos.

V.B. El derecho a borrar

Como desarrollo o precisión del derecho al olvido, Conley propone instituir el derecho a borrar ciertos datos sin importar donde estén registrados o almacenados. Esta potestad estaría limitada a los registros específicos de información –como fotografías o videos– y a aquellos datos que puedan separarse de cualquier expresión de una idea o contenido sin censurarla. Es decir, que se pueda preservar a la vez la libre expresión y la intimidad. «Al hacer posible la eliminación, esperamos que se pueda preservar el derecho a la privacidad y el espacio de oxigenación social que habilita; al hacerlo manual antes que automático, esperamos empoderar a los individuos para controlar su propia información», argumenta Conley.[23]

Bernal, que simpatiza con esta idea, agrega que la presunción debería estar a favor del individuo: éste tiene el derecho a borrar datos asociados a él, mien-

[23] Conley, Chris, «The Right to Delete», en *AAAI Spring Symposium Series,* North America, 2010, disponible en: http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158/1482. p. 54. Traducción informal.

tras que aquellos que deseen preservarlos deben justificar en contrario. Adicionalmente, este autor considera que el derecho a borrar debe incluir los perfiles automáticos de los usuarios, como el historial en los navegadores o motores de búsqueda.

A pesar de defender este derecho, Bernal enumera varias razones por las que es fundamental preservar cierta información más allá del deseo de un individuo de que se elimine: i) por razones paternalistas, cuando es del interés del individuo que la información se preserve (como una historia clínica); ii) comunitarias, cuando existe un interés común de tener ciertos registros (como los antecedentes criminales de alguien); iii) administrativas o económicas, cuando cierta información es fundamental para el funcionamiento institucional (como los registros de votación o de impuestos); iv) de archivo, cuando los datos son necesarios para registrar un hecho histórico (el archivo de las bibliotecas, por ejemplo), y v) de seguridad, que se refieren, entre otros, a la necesidad de retener datos para investigaciones criminales.[24]

El derecho a borrar vendría acompañado por una especie de garantía subsidiaria, que es la «anonimización» de los datos. En los casos en que no fuera posible eliminar el dato, la siguiente obligación sería que éste no permitiera identificar al titular. Este punto es en general pacífico en este debate. De hecho, muchas empresas vienen implementando políticas de «anonimización» de datos. El problema es si el grado de «anonimización» es suficiente para preservar la privacidad del usuario o si, como se referenció anteriormente, permite a la postre identificarlo a medida que la cantidad de datos aumenta.

V.C. ¿Una solución, o un problema?

La propuesta del derecho al olvido de la Comisión Europea ha sido recibida con resistencia entre algunos académicos, activistas y representantes de la industria de Internet. La reacción se evidencia, además, en la diferencia entre la tradición jurídica europea –de donde surge la propuesta– y la tradición jurídica norteamericana –de donde vienen los jugadores más poderosos–.

«El "derecho al olvido" es un eslogan político muy exitoso. Y como todos los eslóganes políticos exitosos, es como un Test de Rorschach[25]. La gente

---

24 Véase Bernal, *supra* nota 8.

25 El Test de Rorschach consiste de una serie de láminas con manchas de tinta con figuras ambiguas que se usan para evaluar la personalidad.

puede ver en él lo que quiera», escribió en enero pasado Peter Fleischer, abogado experto en privacidad y asesor de Google.[26] Recientemente, Fleischer volvió a abordar el tema, esta vez comparando el derecho al olvido con la quema de libros en la antigüedad. Para él, en la práctica, el derecho al olvido permitirá que se oblitere de la red información de interés público:

> «En el mundo real esto puede referirse a cosas como un reporte sobre un policía recibiendo un soborno. O el caso de un doctor enjuiciado por negligencia médica. O una persona iniciando un proceso por bancarrota. Uno puede ver fácilmente cómo la persona en cuestión tiene el interés de borrar toda huella sobre estos hechos vergonzosos, mientras otras personas pueden tener un interés muy legítimo en saber de éstos».[27]

Fleischer subraya el problema de la proporcionalidad y advierte, además, sobre lo que esto puede significar en términos de innovación. Sin comprender aún los usos benéficos que pueden tener estas bases de datos en el futuro –argumenta– decidimos desecharlas por un riesgo que preferimos no ponderar.

Esta necesidad de ponderación y proporcionalidad se ha enmarcado principalmente en la tensión entre el derecho al olvido y la libertad de expresión. Paul Schwartz, director del Centro Berkley para la Ley y la Tecnología, considera que el derecho al olvido, en los términos trazados por la propuesta de la Unión Europea, entraría en conflicto con la Primera Enmienda norteamericana. En particular, Schwartz manifiesta su inquietud por el tipo de responsabilidad de quienes controlan la información inicialmente y de los intermediarios en la cadena sucesiva de transmisión de datos.[28]

Amparada en una protección robusta de la libertad de expresión, la ley norteamericana no contiene disposiciones especiales frente al manejo de informa-

---

[26] Fleischer, Peter, «The right to be forgotten, or how to edit your history» en blog personal, 29 de enero de 2012, disponible en: http://peterfleischer.blogspot.co.uk/2012/01/right-to-be-forgotten-or-how-to-edit.html (consultado en noviembre de 2012). Traducción informal.

[27] *Ibíd.* «Book Burning, udpated for the Digital Age», 14 de noviembre de 2012, disponible en: http://peterfleischer.blogspot.co.uk/2012/11/book-burning-updated-for-digi tal-age.html (consultada en noviembre de 2012). Traducción informal.

[28] Schwartz, Paul, «The E.U.-US Privacy Collision: A Turn to Institutions and Procedures», documento para simposio, 2 de octubre de 2012, disponible en: http://www.har vardlawreview.org/symposium/papers2012/schwartz.pdf.

ción sensible o el proceso automatizado de datos, sino normas generales de responsabilidad civil. Este marco normativo se encuentra, sin duda, en la orilla opuesta del sistema europeo, que no solo contiene normas especiales en materia de datos –como hemos visto–, sino que también permite el establecimiento de controles previos de contenido.[29]

Para Jeffrey Rosen, el derecho al olvido podría convertir a una empresa como Google en un censor de facto antes que una plataforma neutral. «Y como éste es un rol que Google no jugaría» –argumenta– «podría en vez producir hojas en blanco cada vez que un usuario europeo teclee el nombre de alguien que objetó previamente un blog o una actualización de estado desagradables».[30] Siguiendo este planteamiento, el derecho al olvido podría ser también un incentivo para la censura previa.

Recogiendo muchas de estas críticas, algunos autores consideran que para cumplir con el objetivo del derecho al olvido basta con el marco teórico que ofrece el derecho de hábeas data: «el "derecho al olvido" no es nada nuevo; a lo sumo, es simplemente el intento de aplicar a los nuevos mundos de Internet y las tecnologías modernas principios de protección de datos que vienen de tiempo atrás», plantea Fleischer sobre la posición que él suscribe en este debate.[31]

Parece claro que varios de los elementos de la protección de datos –el derecho a rectificar la información personal y la oposición al procesamiento de datos personales sin un objetivo legítimo, entre otros– son parte fundamental del derecho al olvido. Sin embargo, ¿resulta una respuesta adecuada? ¿Ofrece un marco suficiente para procurar soluciones normativas o técnicas?

El caso español ofrece algunas luces para el análisis. Como decíamos anteriormente, la Agencia Española de Protección de Datos ha usado el enfoque

---

29 El artículo 10 de la Convención Europea de Derechos Humanos dispone que la libertad de expresión, «podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial».

30 Rosen, Jeffrey, «The Right to Be Forgotten», *Stanford Law Review* 64, 13 de febrero de 2012, p. 92. Traducción informal.

31 Fleischer, *supra* nota 26.

del hábeas data para garantizar de alguna manera el derecho al olvido. En un caso de 2009, consideró que Google no tenía por qué incluir en el resultado de sus búsquedas o en su memoria «caché» una página que contuviera ciertos datos personales de un individuo. Esto implica que aunque los datos personales podían estar en línea, no habría una manera sencilla de llegar a ellos.[32] Para usar una analogía, una cosa es pescar con red y otra muy distinta, con caña: a partir de ese momento, quien deseara obtener los datos de esa persona necesitaría alguna información precisa para ubicarlos.[33]

En otras oportunidades, la Agencia Española inclinó la balanza hacia el lado contrario. En 2007 y 2009 decidió que la hemeroteca digital de un periódico, la cual puede incluir información específica sobre un individuo, no equivale a la publicación de un dato personal toda vez que no es una base de datos susceptible de tratamiento. Más que hacer un análisis entre los derechos involucrados, el ente oficial simplemente delimitó la frontera de su competencia en un caso particular.[34]

Estos antecedente dan algunos elementos para trazar una caracterización del derecho al olvido y, tal vez, para ponderar los derechos en juego. Sin embargo, parecen insuficiente en varios frentes: se centra en la actuación de intermediarios particulares; restringe el análisis –explicablemente– al tratamiento de datos, dejando de lado la difusión de otro tipo de información en la red; no ofrece respuestas frente a los casos en que el propio afectado publicó la información, y no resuelve los problemas de la automatización de perfiles y la creación de ficheros digitales.

«Las leyes de protección de datos pueden proteger la información de algunos de estos riesgos, pero para la mayoría de ellos resulta efectivamente impotente», dice Paul Bernal.[35] ¿Qué sucede, por ejemplo, con la información

---

32 Véase Cerillo-i-Martínez, Agustí y otros (coords.*), Neutralidad de la red y otros retos para el futuro de Internet*, Actas del VII Congreso Internacional Internet, Derecho y Política, Universitat Oberta de Catalunya, Barcelona, 11-12 de julio de 2011, Universitat Oberta de Catalunya y Huygens Editorial, 2011, p. 376.

33 Para llegar a esa conclusión –acaso consciente de la tensión entre los derechos involucrados–, la Agencia española argumentó que la indexación en buscadores no hace parte de la libertad de información. De lo contrario, tal decisión podría equivaler a una forma de censura.

34 Véase Cerillo-i-Martínez*, supra* nota 32.

35 Bernal*, supra* nota 8.

periodística que, aunque veraz en el pasado, persiste en el presente como información falsa o irrelevante, y que afecta el buen nombre o la integridad de una persona? ¿Qué sucede con la información de un individuo que se mueve en la red sin que el afectado haya consentido o sin que desee que se siga difundiendo? Y, desde un punto de vista más sociológico, ¿podemos reintroducir una forma de olvido que nos permita dejar atrás el pasado, reinventarnos y avanzar?

VI. Olvidar en la práctica

Más allá de que se avance en la creación de un nuevo derecho o en la expansión de uno actual, el ecosistema digital parece requerir de ajustes que permitan enfrentar estos retos. Y tal vez la manera más adecuada de promoverlos no pasa por la imposición de leyes en Internet, lo cual puede resultar imposible a la luz de los estándares internacionales en temas como libertad de expresión y acceso a la información. En América Latina, para hablar de nuestro caso, un esquema de control de contenidos –ya sea para imponerlos o suprimirlos *ex ante*– podría reñir con el artículo 13 de la Convención Interamericana sobre Derechos Humanos, que prohíbe la censura previa y el control posterior en términos razonables.

En vista de este escenario, el gobierno alemán, por ejemplo, hizo un llamado a la autorregulación de los intermediarios,[36] y la propia Agencia Española de Protección de Datos ha promovido esquemas de ese tipo que permitan encontrar un balance:

> «En este sentido los medios de comunicación debieran usar medidas informáticas para que, en el caso de que concurra interés legítimo de un particular y la relevancia del hecho haya dejado de existir, se evite desde su webmaster la indexación de la noticia por los motores de búsqueda en Internet. De esta forma, aun manteniéndola inalterable en su soporte –no se borraría de sus archivos ni de sus históricos– se evitará su divulgación indiscriminada, permanente y, en su caso, lesiva».[37]

---

36 Véase «US Lobbyists Face Off with EU on Data Privacy Proposal», *Der Spiegel*, 17 de octubre de 2012, disponible en: http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html (consultada en noviembre de 2012).

37 Cerillo-i-Martínez, *supra* nota 32, p. 377 (citando a Agencia Española de Protección de Datos, resolución del 26 de enero de 2009).

Las medidas informáticas aludidas se relacionan con el código o la programación del entorno digital. Así como podemos diseñar una casa con varias ventanas y claraboyas para que entre más luz durante el día, podemos diseñar ambientes que permitan «ocupar» el espacio digital de manera diferente; tales cambios en la arquitectura reflejan preocupaciones sociales y buscan cambiar acciones y relaciones. Por supuesto, este código puede cambiar el entorno tanto positiva como negativamente.

La recomendación de la Agencia Española de que algunos sitios de Internet no indexen cierta información es similar a una propuesta hecha por Jonathan Zittrain. El académico norteamericano explica que las «arañas» de los buscadores, encargadas de indexar los contenidos de Internet, revisan el archivo «robots.txt» de todas las páginas web que visitan. Este archivo del «anfitrión» advierte al robot sobre información que no debe indexar.[38] En consecuencia, esta herramienta permitiría, por ejemplo, que ciertos datos personales eventualmente contenciosos dejen de estar al alcance del público en general.

Vale la pena mencionar dos propuestas más que tendrían un efecto directo en la manera como los datos se manejan en el entorno digital: las fechas de vencimiento y la contextualización de la información.

VI.A. Las fechas de vencimiento

Aunque Mayer-Schönberger es considerado por algunos como el promotor del derecho al olvido, su propuesta está más encaminada a introducir un mecanismo práctico que, según él, permita reequilibrar la balanza entre memoria y olvido. «Mi sugerencia es una fecha de vencimiento de la información, para confrontarnos con la finitud de la memoria y exhortarnos a entender (y apreciar) que la información también tiene un ciclo de vida».[39]

En pocas palabras, Mayer-Schönberger propone que los archivos de datos contengan una fecha de expiración, tanto como la tiene una caja de leche, después de la cual se eliminen o queden inservibles. Esto lo haría el propio usuario, quien al momento de crear o compartir el archivo –una foto, por ejemplo– tendría que introducir una fecha de expiración (días, meses o años). Las apli-

---

[38] Véase Zittrain, Jonathan, *The Future of the Internet and How to Stop It,* New Haven y Londres, Yale University Press, 2008, pos. 4447 y ss. (edición Kindle).

[39] Mayer-Schönberger, *supra* nota 2, pos. 290 (edición Kindle). Traducción informal.

caciones del computador y los servicios en línea reconocerían esta información y se encargarían de «limpiar» los datos vencidos –automáticamente, con una frecuencia determinada o a petición del usuario–.

La fecha de vencimiento se convertiría en un elemento esencial del archivo, tanto como su extensión o su nombre. Esto obligaría a que cualquier copia mantenga las características del original y, en este caso, responda al término de vencimiento. La gestión digital de derechos o DRM (*Digital Rights Management*), que condiciona el uso de un contenido a las modalidades permitidas, podría usarse para que las fechas de vencimiento persistan. No obstante, el propio Mayer-Schönberger se muestra escéptico de introducir un sistema automático que elimine la mediación humana, lo cual es en realidad parte del problema: «Después de todo, el objetivo principal de las fechas de vencimiento de la información es precisamente no sacar el problema de la memoria digital de nuestras conciencias al delegárselo a la tecnología».[40]

El autor se refiere a algunas maneras para que se dé el cambio en el código (el ecosistema digital). La Ley podría obligar a que las fechas de vencimiento sean obligatorias –como lo son, por ejemplo, los datos sobre derechos de autor–, lo cual tendría que venir acompañado por una práctica social aceptada. A pesar de esto, y como también reconoce Mayer-Schönberger, las fechas de expiración no podrían resolver todos los problemas relacionados con el uso indebido o desproporcionado de datos personales.

VI.B. La contextualización

La idea de la contextualización (o recontextualización) puede verse como una respuesta a la crítica de Mayer-Schönberger sobre el problema de recordar parcialmente, pero también como una herramienta adicional a las fechas de vencimiento. Detrás de esta propuesta está el argumento de que con la cantidad adecuada de información, tanto el usuario como los terceros que accedan a los datos podrán entender y poner en perspectiva su significado.

En términos prácticos, la contextualización funcionaría en la medida en que el usuario vuelque más información hacia el entorno digital. La fórmula es de alguna manera conocida: combatir la información con más información. Así, si circula por la red un dato injurioso sobre una persona, ésta podría glo-

[40] *Ibídem,* pos. 2820. Traducción informal.

sarlo con información adicional. Se trataría de una forma de réplica para combatir la descontextualización.

Podemos hablar, por un lado, de una propuesta de contextualización o recontextualización extrema, según la cual el ser humano irá paulatinamente registrando todas sus actividades hasta contar con una bitácora digital de su vida. Bajo esta proposición, conocida como *lifelogging*, los beneficios de la abundancia de información superarán las desventajas; entre otras cosas, permitirá poner en contexto cualquier dato personal. «Aun si esto fuera cierto para los individuos», responde Conley, «menos estarán dispuestos a adoptar visiones poco ortodoxas y a retar el *status quo* si toda las ideas y comentarios son grabados y están disponibles de manera permanente».[41]

Por otro lado, podemos hablar de una idea de contextualización moderada, acaso más ajustada al presente. Bajo esta óptica, es posible que los mismos servicios en línea que exponen información personal ofrezcan el espacio para que aquella sea explicada o refutada. «El camino hacia adelante probablemente no es un derecho legal sino una estructura que permita a quienes difunden información construir conexiones con los sujetos de sus discusiones», explica Jonathan Zittrain,[42] quien aboga por un mecanismo de diálogo entre las personas involucradas en el manejo de la información.

En términos más detallados, este sistema podría funcionar mediante la implementación de «etiquetas forzosas» alrededor de la identidad de una persona. En consecuencia, cuando un dato de un sujeto esté en línea, la etiqueta le dará la potestad de proporcionar información adicional.

Esta herramienta puede resultar débil por sí sola. Si se trata, por ejemplo, de una foto humillante que circula en Internet, el afectado no querrá glosarla («es que tomé mucho licor esa noche, entiendan») sino simplemente que se elimine del todo. Zittrain reconoce esta limitación.

De manera dispersa e irregular, algunos sitios de Internet han implementado soluciones que apuntan en la misma dirección de estas propuestas: Google ha dejado de indexar cierto tipo de información en sus buscadores; Disqus ofrece una plataforma de discusión para que los usuarios hagan comentarios en diferentes servicios, lo cual potencia réplicas informales y «curaduría» de

---

41 Conley, *supra* nota 22, disponible en: http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158/1482, p. 54. Traducción informal.

42 Zittrain, *supra* nota 38, pos. 4607. Traducción informal.

contenidos, y Twitter deshecha trinos después de un tiempo determinado. Por supuesto, algunos de estos ejemplos puede tener una cara adversa en términos de acceso a la información y apertura en la red.

Algunas veces han sido los jueces quienes han empujado este cambio, pero en muchos otros casos ha sido el resultado de actores comprometidos con un manejo adecuado de los datos y la información personal. Adicionalmente, el propio mercado ha intentado «corregir» esta situación.

Ambrose explica que sitios como www.reputation.com o www.truerep.com ofrecen servicios para preservar la reputación. Estas empresas se dedican a monitorear la red en busca de información falsa en redes sociales, resultados adversos en motores de búsqueda y uso indebido de datos personales. «El hecho de que estos negocios sean exitosos sugiere que existe un mercado para usuarios injuriados en línea que buscan compensación», afirma Ambrose. Más allá de eso, no parece que la mano invisible vaya a corregir este problema en su totalidad. «Solo aquellos con los medios disponibles pueden eliminarse de los registros de Internet, mientras los menos poderosos solo pueden esperar por una oportunidad para explicar su ropa sucia digital», concluye. Hasta ahí llega el derecho al olvido que ofrece el mercado.

VII. Conclusión y recomendaciones

Antes que resolver el problema del derecho al olvido, este documento se ha dedicado a desempacar las preguntas claves de la discusión. Pero antes de hacerlo, ha tratado de explicar el caso de quienes abogan por una protección nueva frente a los riesgos que genera el flujo incesante de información y datos. Y esa es una conclusión inicial importante: más allá del enfoque que se defienda, la idea del derecho al olvido responde a un problema para el que aún no parece haber una solución. De la misma forma y a manera de recomendación señalamos los siguientes puntos:

- El marco normativo de la protección de datos es, sin duda, un punto de partida para desarrollar la discusión, pero no parece suficiente en el contexto de un entorno digital donde la información tiene formas y modalidades heterogéneas, se origina en múltiples fuentes y trasciende los criterios tradicionales del manejo de bases de datos.
- Por otra parte, la discusión jurídica no puede darse sin tomar en cuenta las fuerzas que moldean e interactúan en el desarrollo de Internet. El mercado, la interacción social y el código –en el sentido informático– son variables ~~interdependientes que definen y habilitan el entorno digital. De esta forma, la~~ existencia de un derecho al olvido puede resultar a la postre indiferente si el

debate jurídico y de política pública no entiende esa dinámica y se alimenta de ella.

• Las propuestas de fechas de vencimiento de datos o de etiquetas personales, por ejemplo, apuntan a un desarrollo tecnológico que no debe pasar desapercibido. Ya sea a través de mecanismos legales o de autorregulación, ideas como estas podrían servir para abordar la propuesta de una especie de derecho al olvido que preserve el equilibrio de los derechos humanos involucrados.

• Sobre esto último, es importante subrayar la tensión en materia de protección de datos y privacidad entre la aproximación europea y la norteamericana. Aunque este documento se centró en esos dos contextos, resulta importante tomar ese antecedente y tener en mente la manera en que esos casos se analizarían a la luz de la Convención Interamericana sobre Derechos Humanos. Siguiendo el artículo 13 de la Convención, que prohíbe la censura previa y propende por controles posteriores proporcionales, no sería un trabajo sencillo adoptar enfoques del derecho al olvido como el que propone la Comisión Europea. Esto obliga a buscar interpretaciones y salidas creativas.

• Un último punto se refiere a los intermediarios. América Latina se encuentra en un momento crucial del debate sobre intermediarios en Internet, ya sea por cuenta del trámite de normas sobre protección de derechos de autor en línea, protección de datos o responsabilidad civil. El análisis del caso del derecho al olvido sugiere que una primera respuesta, tal vez instintiva, es buscar que sean los intermediarios quienes resuelvan los problemas, so pena de ser responsables. Sin embargo, esta aproximación ha generado soluciones dispares y coyunturales, además de ineficientes. Para el caso que nos ocupa, debemos buscar soluciones que abarquen un contexto más amplio; que además de los intermediarios tomen en cuenta a los demás actores involucrados en Internet, empezando por los propios usuarios.

Nombres de dominio: una expresión que merece ser protegida. Recomendaciones y sugerencias para administradores locales de América Latina y el mundo[1]

Resumen

El Sistema de Nombres de Dominio (DNS) es clave para que Internet funcione tal como la conocemos. Sin este sistema, los usuarios deberían aprender y reproducir largas cadenas de caracteres alfanuméricos para acceder a un sitio. Además, los nombres de dominio pueden ser pensados, en sí mismos, como formas de expresión y opinión.

Por lo tanto, todo lo relacionado con el registro o no renovación de estos debería someterse a los estándares que protegen estos derechos fundamentales. De esto se desprende que el diseño institucional de quienes administran los ccTLDs (dominios de nivel superior geográfico) es una cuestión clave.

La Iniciativa por la Libertad de Expresión en Internet (iLEI) del CELE analiza en este documento los distintos modelos que los administradores nacionales de ccTLDs han adoptado. Este trabajo identifica las virtudes y defectos que, desde el punto de vista del ejercicio de la libertad de expresión, presentan, por un lado, el *Modelo de Administración con Alta Injeren-*

[1] Este documento fue elaborado por Eduardo Bertoni, director del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), y Atilio Grimani, asistente de investigación de la Iniciativa por la Libertad de Expresión en Internet (iLEI), con la contribución de Carlos Cortés Castillo, investigador del iLEI. Agradecemos a Alejandro Pisanty, del Departamento de Física y Química Teórica, Facultad de Química, UNAM, México, y Presidente de la Sociedad Internet de México, A. C., México D. F., por sus comentarios y aportes en la realización de este trabajo.

cia Estatal y, por otro, el de *Múltiples Partes Interesadas,* que cuenta con participación de la sociedad civil. Asimismo, analiza, en particular, el caso argentino.

Al final del documento, se presentan una serie de recomendaciones para los Estados y organismos administradores a fin de que la asignación de nombres de dominio vaya en consonancia con los estándares internacionales en materia de derechos humanos en línea.

I. Introducción

Probablemente muy pocas personas en el mundo de hoy desconocen qué es una página web[2]. El uso extendido de Internet ha generado que ante tal pregunta surjan a modo de respuesta un sinnúmero de nombres, como Amazon, Google y Yahoo. Para la mayoría de los usuarios, eso es todo lo que es necesario saber sobre Internet. Esos nombres son lo que nos facilita el acceso a una cantidad de información de diversa índole que parece no tener límites. El usuario ingresa el nombre de la página que desea acceder en su navegador –Internet Explorer, Chrome, Safari– o en un buscador de Internet –Google, Yahoo, Bing, etc.– y eso es todo. Sencillo, ¿verdad? Sin embargo, existe mucho más de lo que a simple vista se puede ver.

Parecería ridículo que para acceder a un sitio el usuario tuviese que aprender y reproducir en su computadora una larga cadena de números o de caracteres alfanuméricos, como 173.194.42.19 para Google, o 72.21.214.128 para Amazon. Un esfuerzo de este calibre desalentaría a la mayoría de los usuarios y atentaría con la lógica de libre acceso que ha hecho de Internet lo que es hoy. Para funcionar de la manera en que lo hace, Internet precisa de estos nombres que nos dirigen a donde queremos ir con sólo ingresarlos a través de nuestro teclado en la computadora. Las computadoras se hacen cargo del resto.

La forma en la que internamente se maneja este proceso es a través de lo que se llama Sistema de Nombres de Dominio o DNS. El DNS es un sistema que permite, entre otros, hacer el mapa entre un nombre de dominio y una dirección IP de manera unívoca. El DNS funciona de manera jerárquica y des-

---

2 Según las últimas estadísticas de la Unión Internacional de Telecomunicaciones (ITU), hacia fines de 2011 había 2.3 billones de personas online, disponible en: http://www.itu.int/ITUD/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf (consultada el 10 de septiembre de 2012).

centralizada: jerárquica porque está organizado en niveles –siguiendo el mismo principio de diseño de Internet– y descentralizada porque el directorio no reside en un único sitio central sino que está asignado, por partes, a diversos nodos de la red. De esta forma, puede ser visto como un árbol con ramas que habitualmente llegan a tener hasta cuatro o cinco niveles, empezando por la «raíz», siguiendo con los dominio de primer nivel (TLD o *Top Level Domains*), y de ahí sucesivamente hasta formar la estructura completa.

La forma en que opera este sistema es mediante delegación de autoridad. Así, el registrante y operador de un *Generic Top Level Domain* o gTLD, por ejemplo «.com», es responsable de mantener disponible, mediante equipos conocidos como servidores de nombres, las asociaciones existentes entre un nombre de dominio registrado y una dirección IP determinada. Por otra parte, cuenta con total libertad para crear y asignar dichos nombres mientras éstos cumplan con los estándares técnicos. Este sistema altamente descentralizado ha resultado extraordinariamente escalable y robusto, características que son parte de las causas de la rápida expansión mundial de Internet, que sigue avanzando sin detenerse.

De esa forma, cuando hablamos de «Google.com» o «Amazon.com» nos referimos a nombres de dominios particulares que hacen parte del sistema general –el DNS–. Estos nombres son únicos a nivel global y están relacionados con esas cadenas numéricas referidas anteriormente, llamadas direcciones IP. Son estas direcciones IP las que nos marcan el lugar donde está el sitio web al que queremos acceder. Es decir, que identifican a todos los computadores que se conectan a la red (incluido el nuestro). Si bien parecen incomprensibles, no son muy distintas de las direcciones de nuestros hogares. Si la dirección en cuestión fuese «173.194.42.19», 173 podría ser el código asignado al país; 194 el número de un proveedor de acceso a Internet o ISP (Fibertel en Argentina, VTR en Chile, Telmex en México, etc.); 42 el número asignado al servicio informático y 19 la dirección que se le ha asignado a la máquina.[3]

Los nombres de dominio no solamente se refieren a páginas web; identifican recursos en Internet para todos los protocolos, incluyendo entre los más conocidos el correo electrónico, FTP para copiar archivos hacia o desde servidores, acceso remoto a computadoras y voz sobre IP. En términos generales, la función que cumplen es la misma: identificar la dirección de IP con un ser-

---

[3] Molina Quiroga, E., *Tratado Jurisprudencial y Doctrinario. Derecho Informático*, t. I, 1ª ed., Buenos Aires, La Ley, 2011, p. 251.

vicio determinado en la red. Los nombres de dominio también aparecen, en formas peculiares, asociados con algunos usos maliciosos de Internet, para los cuales se registran miles de nombres de dominio de manera sucesiva para ser utilizados solamente durante un breve intervalo en la coordinación y ejecución de tipos muy agresivos de ataques informáticos. Igualmente, hacen parte de un mercado especulativo –y frecuentemente abusivo–, ya que tienen indudable valor comercial. Así, un tercero se hace a un paquete de dominios atractivos («turismo.com», por ejemplo), y los comercializa como si se tratara de bienes raíces.

Con algo más de 600 millones de sitios web activos en el mundo,[4] es claro que los nombres de dominio están ahí para hacer nuestra vida más fácil. Sin embargo, un número tan elevado de páginas requiere de algún tipo de control o coordinación. Esta tarea es realizada en la actualidad por la Corporación de Internet para la Asignación de Nombres y Números (ICANN, por sus siglas en inglés). Así, el DNS tiene un único punto que requiere coordinación central, a saber, la raíz del DNS. Esta consiste en un directorio que contiene las asociaciones entre los nombres de dominio de primer nivel (indistintamente ccTLDs o gTLDs), los datos de las direcciones IP de sus respectivos servidores de nombres y las personas responsables de su operación técnica y administrativa. La operación de la raíz del DNS está bajo responsabilidad de un departamento de ICANN llamado IANA (ver *infra*). Y las políticas generales para la operación de IANA y para la evolución del DNS, más allá de los estándares técnicos que son responsabilidad de la Internet Engineering Task Force (IETF), residen en ICANN.

ICANN es una organización no lucrativa de naturaleza privada que fue creada en 1998. Ese mismo año, el Ministerio de Comercio de Estados Unidos emitió un *White Paper*[5] sobre la administración de los nombres y números de Internet. Su propósito era pasar la administración de los nombres de dominio de Internet y de las direcciones IP, del gobierno federal de los Esta-

---

4 Netcraft, «September 2012 Web Server Survey», disponible en: http://news.netcraft.com/archives/2012/09/10/september-2012-web-server-survey.html (consultada el 10 de septiembre de 2012).

5 Department of Commerce, NTIA, «Management of Internet Names and Addresses», Statement of Policy, Federal Register, Vol. 63, N° 111, 10 de junio de 1998, p. 31741, disponible en: http://www.ntia.doc.gov/files/ntia/publications/6_5_98dns.pdf (consultada el 10 de septiembre de 2012).

dos Unidos[6] a las manos de una entidad privada sin fines de lucro que estuviese representada internacionalmente. Esta función era desarrollada hasta ese momento por la Autoridad de Internet para la Asignación de Números o IANA. A fines de 1998, el Ministerio de Comercio reconocería a ICANN como la entidad que pasaría a cumplir estas funciones;[7] IANA continuaría realizando esta tarea, funcionando dentro de la estructura de ICANN.

Entre otras tareas, ICANN se encarga de definir políticas sobre la forma en que el sistema debería funcionar y de coordinar, a nivel mundial, la arquitectura del DNS. ICANN coordina las direcciones IP y la administración del sistema de nombre de dominio de alto nivel, tanto genéricos (*generic Top Level Domains* o gTLD, que se refiere, por ejemplo, al «.com» a la derecha de los diferentes nombres) como de códigos de países[8] (*country code Top Level Domanis* o ccTLD, se refiere, por ejemplo en Argentina, a los «.com.ar»).[9] Sin esta tarea de coordinación, Internet no podría ser «una» a nivel global.

---

[6] El gobierno de Estados Unidos tuvo un papel fundamental en los comienzos de Internet, prestando fondos para las investigaciones necesarias, comenzando con redes como ARPANET, la cual fue establecida por el Ministerio de Defensa de Estados Unidos. Las distintas funciones colectivas que se realizaban para el mantenimiento de las listas de números y nombres asignados se transformaron eventualmente en lo que sería la Autoridad de Internet para la Asignación de Números. Para más información sobre este tema ver Department of Commerce, NTIA, «Management of Internet Names and Addresses», Statement of Policy, Federal Register, Vol. 63, N° 111, 10 de junio de 1998, p. 31741, disponible en: http://www.ntia.doc.gov/files/ ntia/publications/6_5_98dns.pdf (consultada el 10 de septiembre de 2012).

[7] Department of Commerce, NTIA, «Memorandum of Understanding between the U.S. Departement of Commerce and the Internet Corporation for Assigned Names and Numbers», disponible en: http://www.ntia.doc.gov/page/1998/memorandum-understanding-between-us-department-commerce-and-internet-corporation-assigned- (consultada el 10 de septiembre de 2012).

[8] ICANN, «What does ICANN do?», disponible en: http://www.icann.org/en/about/welcome (consultada el 10 de septiembre de 2012).

[9] A diferencia de lo que se podría pensar, los ccTLD no son dependientes de los gTLD, sino que se encuentran en el mismo nivel jerárquico. Tampoco se encuentran incluidos unos dentro de los otros. Los gTLD, como su nombre lo indica, son genéricos. Es decir que son comunes a toda la comunidad de Internet. Entre ellos podemos encontrar los .com, .org, .net, .biz, etc. Los ccTLD, en cambio, emanan de un código de origen geográfico y se refieren a cada uno de los países en cuestión, a la vez que son organizados por un administrador de cada país. Así hablamos de .com.ar, .org.br, .biz.uy. Para una idea más profunda sobre este tema, ver Request for Comments N° 1591, «Domain Name System Structure and Delegation», disponible en: http://tools.ietf.org/rfc/rfc1591.txt (consultada el 10 de septiembre de 2012).

Pero ICANN no se encarga personalmente de la administración y asignación de todos los gTLDs y ccTLDs –esto significaría una utilización de recursos enorme y un avasallamiento de las jurisdicciones nacionales– sino sólo de su coordinación general, como se ha descrito arriba. En su lugar y desde el comienzo, estas funciones de administración y asignación fueron delegadas a empresas privadas, en el caso de los gTLDs, y a una variedad de organismos en el caso de los ccTLDs[10] Estos administradores, en las palabras de unos de los «padres fundadores» de Internet y del Sistema de Nombres de Dominio en particular, llevan a cabo un servicio público en beneficio de la comunidad de Internet.[11]

En lo que respecta a los ccTLDs, los organismos administradores de cada uno de los países se organizan, debido al rol que juegan en el desarrollo de sus políticas los gobiernos nacionales,[12] en formas muy dispares,[13] lo cual podría traer tanto beneficios como problemas desde una visión de la libertad de expresión en Internet. Como establecimos en los párrafos precedentes, la función de la administración de los nombres de dominio es de fundamental importancia para que Internet funcione de la manera en que lo hace y para que los sitios puedan ser encontrados por los usuarios. La injerencia negativa de un estado nacional al momento de la asignación o renovación de éstos puede causar un perjuicio para los usuarios y propietarios de los mencionados dominios.

A lo largo de este documento analizaremos los distintos modelos por los que los administradores nacionales de ccTLDs han optado en el mundo, extendiéndonos particularmente en el caso argentino. Identificaremos lo que

---

[10] Para una lista de todos los administradores de TLDs, ver «Root Zone Database», disponible en: http://www.iana.org/domains/root/db/ (consultada el 10 de septiembre de 2012).

[11] Postel, J., Request for Comments N° 1591, «Domain Name System Structure and Delegation», disponible en: http://tools.ietf.org/rfc/rfc1591.txt (consultada el 10 de septiembre de 2012).

[12] Department of Commerce, NTIA, «Management of Internet Names and Addresses», Statement of Policy, Federal Register, Vol. 63, N° 111, 10 de junio de 1998, p. 31742, disponible en: http://www.ntia.doc.gov/files/ntia/publications/6_5_98dns.pdf (consultada el 10 de septiembre de 2012).

[13] Postel, J., Request for Comments N° 1591, «Domain Name System Structure and Delegation», disponible en: http://tools.ietf.org/rfc/rfc1591.txt. También, «Root Zone Database», disponible en: http://www.iana.org/domains/root/db/ (consultadas el 10 de septiembre de 2012).

creemos son, desde el ejercicio de la libertad de expresión, defectos y virtudes de estos modelos, procurando hacia el final dar recomendaciones que tiendan a establecer una práctica de asignación de nombres de dominio que vaya en consonancia con los distintos principios relativos a los derechos humanos en línea enarbolados por usuarios, numerosas organizaciones y gobiernos.

II. ICANN, IANA y los ccTLDS

Como dijéramos, se les confía el manejo de los ccTLDs de cada país a los distintos organismos administradores.[14] Sin embargo, incluso esta primera tarea encierra previamente la dificultad y posible controversia acerca de tener que tomar la decisión sobre qué países son elegibles para ostentar un ccTLD. El RFC 1591, que rige en gran medida la operación de IANA, dice inequívocamente: «no nos toca decidir qué es un país y qué no lo es». ICANN no es el encargado –tampoco lo es IANA– de zanjar esta discusión, al menos no directamente. En su lugar, la selección se realiza utilizando la lista 3166-1,[15] estandarizada y neutral, confeccionada por la Agencia de Mantenimiento ISO 3166,[16] en la que se le asigna a cada país incluido un código de dos letras.

La Agencia de Mantenimiento ISO 3166 es la encargada de mantener actualizada la lista de países, la cual fue publicada por primera vez en 1974. El método para ser incluido en la lista 3166-1 consiste en estar inscripto, ya sea en el Boletín de Terminología de Nombres de Países de las Naciones Unidas o en la lista de Códigos de Países y Regiones para Uso Estadístico de las Naciones Unidas.[17] A su vez, para poder ser incluido en estas listas de Nacio-

---

[14] Estos organismos también son llamados operadores de registro o centros de información de la red (NIC, por sus siglas en inglés). Es importante no confundir a estos NIC con las organizaciones patrocinadoras bajo cuya órbita aquellos funcionan. Así, en Argentina nos encontramos con una organización patrocinadora, la Presidencia de la Nación –Secretaría Legal y Técnica– y con un operador de registro, NIC.ar.

[15] Lista 3166-1, International Organization for Standardization (ISO), disponible en: http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm (consultada el 17 de septiembre de 2012).

[16] Country Codes - ISO 3166, International Organization for Standardization (ISO), disponible en: http://www.iso.org/iso/country_codes (consultada el 17 de septiembre de 2012).

[17] «Países o áreas, códigos y abreviaturas», Naciones Unidas, disponible en: http://unstats.un.org/unsd/methods/m49/m49alpha.htm (consultada el 17 de septiembre de 2012).

nes Unidas es necesario ser miembro de la Organización de las Naciones Unidas, miembro de una de sus agencias especializadas o parte del Estatuto de la Corte Internacional de Justicia.[18] Cabe mencionar que entre los 10 miembros con derecho a voto de la Agencia de Mantenimiento ISO 3166, se encuentran incluidos la Unión Internacional de Telecomunicaciones (ITU) e ICANN.[19]

Una vez aclarado qué países serán considerados para obtener un ccTLD –y el porqué de esta selección–, ICANN establece un proceso interno para la delegación o redelegación de un ccTLD en manos de un operador o administrador.[20] Este proceso será llevado adelante por IANA. Los involucrados en este proceso son, entre otros posibles, i) el nuevo operador propuesto, quien inicia el proceso y provee la información necesaria; ii) la organización patrocinadora, en la mayoría de los casos los gobiernos asociados, quienes verifican el apoyo a la delegación; iii) las distintas partes a las que el ccTLD preste un servicio, a quienes se les pide que muestren su apoyo y expliquen en qué forma esta delegación cumple las necesidades e intereses de la comunidad local de Internet; iv) el personal de IANA encargado de la administración de la raíz, actuando como coordinador y analista de la propuesta, que prepara una recomendación para la Junta de ICANN; v) la junta de directores de ICANN, que consideran la recomendación preparada por IANA y votan si la propuesta debe avanzar; y vi) el Ministerio de Comercio de los Estados Unidos, que evalúa un reporte realizado por IANA.[21]

---

[18] IANA, «Procedimiento para establecer ccTLDs», disponible en: http://www.iana.org/pro cedures/cctld-establishment.html (consultada el 17 de septiembre de 2012).

[19] «How ISO 3166 is maintained. International Organization for Standardization (ISO)», disponible en: http://www.iso.org/iso/country_codes (consultada el 17 de septiembre de 2012).

[20] En el comienzo, con la implementación de los primeros ccTLDs, esta función fue muchas veces confiada a personas físicas específicas, algunas veces conocidos personales de Jon Postel, quien los designaba personalmente. Estas personas podían ser, por ejemplo, profesores en universidades de ingeniería que contaban con los recursos para realizar dicha tarea o aquellos pioneros que estaban experimentando con Internet en un país determinado. Hoy en día, sin embargo, esta función es realizada en su mayoría por organizaciones. En IANA, «Submitting the Request», disponible en: http://www.iana.org/domains/root/delegation-guide/ (consultada el 17 de septiembre de 2012). También, para ver el caso canadiense, en «Framework for the administration of the .ca domain name system», disponible en http://www.cira.ca/assets/Documents/Publications/CDNCC report.pdf, p. 6 (consultada el 17 de septiembre de 2012).

[21] IANA, «Who is involved in a delegation or redelegation», disponible en: http://www.iana.org/domains/root/delegation-guide/ (consultada el 17 de septiembre de 2012).

La inclusión de las diferentes partes y la documentación que se acompaña a la hora de la presentación responde a una variedad de intereses de importancia. El principio que guía a los ccTLDs, siempre de acuerdo con el RFC 1591, es servir tanto a la Comunidad Global de Internet como a la Comunidad Local de Internet (LIC), haciendo posible encontrar los recursos en la red que estén identificados con nombres de dominio por los que el administrador deba responder. Así, la mayor preocupación a la hora de designar un administrador para un dominio se relaciona con su capacidad técnica y administrativa para llevar a cabo las responsabilidades que sean necesarias para la consecución de su labor, sumado a la habilidad de hacerlo en una forma justa, honesta, equitativa y competente. La documentación proporcionada debe reflejar estas cualidades. Es necesario comprender que estos administradores han sido confiados con el manejo del dominio y tienen el deber de servir a la comunidad en su conjunto, incluso a nivel mundial.[22] Consecuentemente, las opiniones y deseos del gobierno del país que se trate son tomados muy en serio y forman una parte muy importante del proceso decisorio de ICANN.[23] De igual manera, la opinión de la comunidad local de Internet es crucial.[24/25]

Sin embargo, esto no implica que todos los administradores de ccTLDs deban tener las mismas políticas y procedimientos internos. Ambos deben estar documentados y ser asequibles para la inspección pública de la comunidad a cuyos intereses sirven. Y si bien se espera un trato justo y equitativo hacia todo aquel que requiera un nombre de dominio, aplicando siempre las mismas reglas de una manera no discriminatoria, éstas pueden variar de un

---

22 Postel, J., Request for Comments N° 1591, «Domain Name System Structure and Delegation», disponible en: http://tools.ietf.org/rfc/rfc1591.txt (consultada el 10 de septiembre de 2012).

23 IANA, «CCTLD News Memo N° 1», 23 de octubre de 1997, disponible en: http://www.iana.org/reports/1997/cctld-news-oct1997.html (consultada el 17 de septiembre de 2012).

24 Ejemplos del tipo de documentación esperada incluyen declaraciones de ISP nacionales, grupos de usuarios de Internet, titulares de propiedad intelectual, entre otros. IANA, «Submitting the Request», disponible en: http://www.iana.org/domains/root/delegation-guide/ (consultada el 17 de septiembre de 2012).

25 Para ver un ejemplo de reporte sobre delegación del dominio .me, ver http://www.iana.org/reports/2007/me-report-11sep2007.html (consultada el 18 de septiembre de 2012).

país a otro en función de las costumbres locales y valores culturales.[26] Así, existen políticas propias de cada operador, adaptadas para satisfacer las circunstancias económicas, culturales y lingüísticas específicas de cada país o territorio.[27]

III. Modelos de administración de ccTLDs

Los distintos administradores de ccTLDs del mundo comparten distintas funciones, responsabilidades y atribuciones, y deben cumplirlas adecuadamente y en sintonía con los preceptos mencionados en la sección anterior. Entre ellas podemos mencionar funciones básicas de registro,[28] servicios a los miembros,[29] servicios a los registrados,[30] servicios a las entidades registrantes[31] y representación del dominio en los foros pertinentes.[32] La mala administración, la violación de las políticas establecidas por ICANN o los problemas recurrentes con el correcto funcionamiento del dominio, habilitan a

[26] ICANN, «ICP-1: Internet Domain Server System Structure and Delegation», disponible en: http://www.icann.org/en/resources/cctlds/delegation (consultada el 17 de septiembre de 2012).

[27] ICANN, «ccTLD Delegation and Administration Policies», disponible en: http://archive.icann.org/en/meetings/cairo2000/cctld-topic.htm (consultada el 18 de septiembre de 2012).

[28] Servicios de búsqueda en línea en la base de datos del dominio, servicios de resolución de nombres de domino, administración y mantenimiento de la base de datos, etcétera.

[29] Algunos modelos de administración contemplan la inclusión como miembros de sus registrados. A ellos se les presta distintos servicios, como por ejemplo la creación y distribución de información para los miembros, reportes financieros, reuniones anuales, etcétera.

[30] Incluyendo servicios de resolución alternativa de disputas, resolución de disputas entre los registrados y las entidades que los registran, etcétera.

[31] Algunos modelos de administración delegan en distintas entidades la función de registración propiamente dicha. A estas entidades se les provee servicios de listado de entidades, resolución de disputas entre los registrados y las entidades, etcétera.

[32] Hemos tomado como modelo para confeccionar este pequeño detalle las funciones del administrador del ccTLD de Canadá, CIRA, «Framework for the administration of the .CA domain name system», disponible en: http://www.cira.ca/assets/Documents/Publications/CDNCC-report.pdf (consultada el 17 de septiembre de 2012), p. 10.

IANA a revocar y redelegar el control del dominio a otro administrador.[33] Aun así, siempre ha estado contemplado que los distintos administradores de ccTLDs se organicen de diferente forma, tanto a nivel administrativo como a nivel técnico.[34] En lo que a esto refiere, ICANN solo requiere que esta organización y sus reglas particulares estén documentadas y disponibles, por ejemplo en las páginas web de los administradores.

Los distintos entes administradores de registro pueden moldearse de distintas formas, permitiendo diversos niveles de injerencia estatal. De esta forma podemos observar modelos que se encuentran directamente debajo de la órbita del Ejecutivo y otros en los que el Estado no es *per se* quien dicta las políticas a seguir. En medio de estos dos extremos existen una infinidad de variantes.

III.A. Modelos con alta injerencia estatal

Existen modelos donde la administración del ccTLD se encuentra bajo la órbita directa del gobierno y sin participación de la sociedad civil interesada en el desarrollo de Internet y en la defensa de los derechos de sus usuarios. En Venezuela, por ejemplo, la organización patrocinadora es la Comisión Nacional de Telecomunicaciones (CONATEL),[35] un organismo que depende del Ministerio del Poder Popular para las Telecomunicaciones y la Informática. Es CONATEL quien administra y gestiona al «NIC.ve». Inicialmente esta función había sido encomendada por el ICANN al Consejo Nacional de Investigaciones Científicas y Tecnológicas (CONICIT). Esta era una organización venezolana conectada a Internet, en la cual se agrupaba la mayor parte del sector académico, científico y de investigación del país. La entidad encargada de la administración y la gestión técnica del «.ve» en CONICIT era el Servicio Automatizado de Información Científica y Tecnológica (SAICYT)

---

33 ICANN, «ICP-1: Internet Domain Server System Structure and Delegation», disponible en: http://www.icann.org/en/resources/cctlds/delegation (consultada el 17 de septiembre de 2012).

34 Postel, J. Request for Comments N° 1591, «Domain Name System Structure and Delegation», disponible en: http://tools.ietf.org/rfc/rfc1591.txt (consultada el 10 de septiembre de 2012).

35 IANA, «Delegation Record for .ve», disponible en: http://www.iana.org/domains/root/db/ve.html (consultada el 18 de septiembre de 2012).

Eventualmente, el proyecto SAICYT se transformó en la Red Académica de Centros de Investigación y Universidades Nacionales (REACCIUN), organización fundada por el CONICIT y 13 universidades nacionales, que comenzó a operar en 1995 y asumió las responsabilidades que tenía SAICYT entre las cuales incluía la administración del nombre de dominio «.ve». El 22 de marzo de 2000, se creó por decreto presidencial el Centro Nacional de Tecnologías de Información, el cual asumió el capital humano y la plataforma que poseía REACCIUN.[36]

En este caso, es el mismo CONATEL a través del Centro de Información de Red de Venezuela («NIC.ve») quien se encarga de realizar los registros. Si bien no parece haber limitaciones especiales en cuanto al registro de dominios, la suspensión o eliminación de éstos incluye dentro de sus razones, además de la falsedad en cuanto a los datos proporcionados y el incumplimiento de los pagos, la solicitud por parte de cualquier autoridad competente.[37] En numerosas ocasiones, CONATEL ha demostrado ser adepta a los requerimientos del gobierno venezolano a la hora de suspender señales televisivas de aire opositoras.[38] Incluso se ampliaron sus poderes para sancionar emisoras de radio y TV, así como a los medios electrónicos que violasen las restricciones existentes a la libertad de expresión, permitiéndole suspender o revocar las concesiones cuando considerase tal decisión fuese «conveniente a los intereses de la Nación».[39]

---

36 Centro de Información de Red de la República Bolivariana de Venezuela, «Historia», disponible en: http://www.nic.ve/noticias/bienvenida (consultada el 18 de septiembre de 2012).

37 CONATEL, «Condiciones de registro de nombres de dominio», disponible en: http://www.nic.ve/uploads/7i/iJ/7iiJjw8PBlT9U1Al9alXng/condiciones_nic_ve.pdf (consultada el 18 de septiembre de 2012).

38 En este sentido, los casos de Radio Caracas Televisión (RCTV) y Globovisión. El primero sufrió la no renovación de su concesión y debió interrumpir la transmisión en frecuencias abiertas en mayo de 2007. El segundo sufrió la imposición de una multa millonaria y se enfrenta a nuevas investigaciones que podrían resultar en nuevas multas e incluso en la suspensión de la transmisión o la revocación de su habilitación y concesión. En Human Rights Watch, «Concentración y abuso de poder en la Venezuela de Chávez», julio de 2012, ps. 54 y 58, respectivamente, disponible en: http://www.hrw.org/sites/default/files/reports/venezuela0812sp.pdf (consultada el 1 de octubre de 2012).

39 Human Rights Watch, «Concentración y abuso de poder en la Venezuela de Chávez», julio de 2012, p. 52, disponible en: http://www.hrw.org/sites/default/files/reports/venezuela 0812sp.pdf (consultada el 1 de octubre de 2012).

Otro ejemplo de este tipo de modelos podría ser, aunque con algunas variaciones, China. En este país, la organización patrocinadora es la Academia de Ciencias China (CAS),[40] la cual depende del Ministerio de Industria Informática de China. Dentro de la CAS encontramos el CNNIC, una organización estatal sin fines de lucro, encargada de administrar el dominio «.cn» (todo debe ser informado al Ministerio y aprobado por éste). El *CNNIC Steering Committee*, un grupo compuesto por expertos reconocidos y representantes comerciales de la comunidad de Internet doméstica, supervisan y evalúan la estructura, la operación y la administración de CNNIC.[41]

En lo referente a lo que está permitido a la hora de hacer uso de un dominio «.cn», el artículo 27 de las Regulaciones referente a los Nombres de Dominio de Internet en China estipula varias restricciones que hacen referencia, entre otras, a la Constitución, a la seguridad nacional, al honor e intereses nacionales, religión, estabilidad social, la pornografía, calumnias, obscenidad y todo contenido prohibido en leyes, reglas y reglamentaciones administrativas en general.[42] El artículo 19 de la Implementación de las Reglas de Registración de Nombres de Dominio del CNNIC estipula que la violación de las restricciones mencionadas acarrea la cancelación del dominio en cuestión.[43]

III.B. Modelos con injerencia de múltiples partes interesadas

En estos casos, el administrador de registro se encuentra conformado por miembros del Estado –en mayor o menor medida– pero también con miembros de la sociedad civil involucrada de cerca con Internet y su desarrollo. En el caso de Brasil, «NIC.br» es una entidad civil sin fines de lucro que implementa las decisiones del CGI.br (Comité Gestor de Internet), una entidad mixta constituida por representantes del gobierno, el sector privado lucrativo,

---

40 «IANA, «Delegation Record for .cn», disponible en: http://www.iana.org/domains/root/ db/cn.html (consultada el 18 de septiembre de 2012).

41 CNNIC, «A brief introduction of CNNIC», disponible en: http://www1.cnnic.cn/en/index/0Q/index.htm (consultada el 18 de septiembre de 2012).

42 CNNIC, «China Internet Domain Name Regulations», disponible en: http://www1.cnnic. cn/html/Dir/2005/03/24/2861.htm (consultada el 18 de septiembre de 2012).

43 CNNIC, «Implementing Rules of Domain Name Registration», disponible en: http://www1.cnnic.cn/html/Dir/2012/05/28/6043.htm (consultada el 18 de septiembre de 2012).

sociedad civil y un experto en Internet. El CGI.br es la organización promotora[44] y tiene el propósito de coordinar e integrar todas las iniciativas de servicio de Internet en Brasil, promoviendo la calidad técnica, innovación y diseminación de los servicios disponibles.

NIC.br es el brazo ejecutivo del CGI.br y su conformación no puede ser separada la una de la otra. Así, la estructura orgánica de ambos se confunde. El CGI.br está conformado por 21 miembros, de los cuales 9 son representantes del gobierno –de distintos ministerios, agencias, etc.-, 11 representan a la sociedad civil –4 del sector empresarial, 4 del tercer sector y 3 de la comunidad científica y tecnológica–, y un experto en Internet. El mandato de los miembros de la sociedad civil es de dos años y serán elegidos por el voto de distintos colegios electorales conformados por representantes de entidades pertenecientes cada segmento involucrado.[45]

A su vez, NIC.br está gobernado por una Asamblea General cuyos miembros son miembros o ex miembros de CGI.br.[46] Es importante destacar que el patrimonio y los recursos con los que cuenta NIC.br son propios, obtenidos a través de donaciones, de convenios y contratos en los que participa y de las actividades financieras correspondientes.[47] Una curiosidad de este sistema es que NIC.br realiza la función de registro y mantenimiento de dominios «.br» a través de REGISTRO.br,[48] uno de los cinco departamentos por medio de los cuales NIC.br lleva a cabo sus funciones.[49]

---

44 IANA, «Delegation Record for .br», disponible en: http://www.iana.org/domains/root/db/br.html (consultada el 18 de septiembre de 2012).

45 Ministerio de Comunicaciones, Orden Interministerial N°147, 31 de mayo de 1995, disponible en: http://www.cgi.br/regulamentacao/port147.htm (consultada el 1 de octubre de 2012). También, Presidencia de la República de Brasil, Decreto N° 4.829, 3 de septiembre de 2003, disponible en: http://www.cgi.br/regulamentacao/decr4829.htm (consultada el 1 de octubre de 2012).

46 NIC.br, «Quem Somos», disponible en: http://www.nic.br/sobre-nic/nicbr.htm (consultada el 1 de octubre de 2012).

47 NIC.br, «Estatuto de NIC.br», disponible en: http://www.nic.br/estatuto/index.htm (consultada el 1 de octubre de 2012).

48 Disponible en http://registro.br/ (consultada el 18 de septiembre de 2012).

49 Para más información al respecto de la organización de CGI.br, NIC.br y sus departamentos asociados, ver http://www.nic.br/english/about/nicbr.htm (consultada el 18 de septiembre de 2012).

En cuanto a las regulaciones referentes a la cancelación de una concesión de un dominio, el artículo 9 de la Resolución N° 2008/008/P del CGI.br estipula diferentes causales entre las que se encuentran una orden judicial o la constatación de irregularidades en los datos ofrecidos y la no rectificación de éstos una vez solicitada su corrección por parte de NIC.br. Esta notificación será realizada por medio de un contacto administrativo, para que en el plazo de 14 días se reviertan las irregularidades.[50]

En Canadá, la administración del registro es llevada a cabo por la Autoridad de Registro de Internet Canadiense (CIRA) oficialmente desde 2000. Anteriormente, la labor era realizada por el Departamento de Ciencias de la Computación de la Universidad de Columbia Británica (UBC).[51] El «*Framework for the administration of the .CA domain name system*» fue la base para la transición de la UBC al CIRA. En este documento se especifica cómo, por razones históricas, fue Jon Postel quien le delegó personalmente el manejo de «.ca» a John Demco. Él y su equipo, con ayuda del Comité de «.ca», fueron quienes voluntariamente asignaron dominios «.ca» en forma gratuita desde el comienzo. Sin embargo, debido a las fallas y retrasos en el servicio, la comunidad de usuarios de Internet decidió crear el CDNCC (*Canadian Domain Name Consultant Committee*) que en diciembre de 1998 dio lugar a la creación de CIRA.[52]

Curiosamente, y debido quizás a la historia particular de CIRA, es esta misma organización la que aparece como organización promotora.[53] También llama la atención la estructura interna que ostenta. El órgano de gobierno es una junta de directores conformada por 15 personas, 12 de las cuales son electas por los miembros de CIRA y 3 son directores ex oficio sin derecho a voto. Entre estos últimos se encuentran el presidente de CIRA, un representante del

---

50 CGI.br, «Resolución 2008/008/P - Procedimientos para registro de nombres de dominio», disponible en: http://www.cgi.br/regulamentacao/resolucao2008-008.htm (consultada el 18 de septiembre de 2012).

51 CIRA, «About CIRA», disponible en: http://www.cira.ca/about-cira/history/ (consultada el 18 de septiembre de 2012).

52 CIRA, «Framework for the administration of the .CA domain name system», disponible en: http://www.cira.ca/assets/Documents/Publications/CDNCC-report.pdf (consultada el 18 de septiembre de 2012).

53 IANA, «Delegation Record for .ca», disponible en: http://www.iana.org/domains/root/db/ca.html (consultada el 18 de septiembre de 2012).

gobierno canadiense y John Demco, quien cumpliría la función de experto en Internet.[54] En cuanto a los miembros, para aplicar a la membresía basta con tener un dominio «.ca» activo.[55] De esta manera, son los propios usuarios quienes indirectamente tienen poder para tomar una decisión respecto del futuro de los negocios en Internet y de ésta como espacio cultural.[56] Financieramente, CIRA opera desde sus comienzos con un modelo de recuperación de costos (*cost-recovery basis*) que le permite cumplir sus objetivos.[57]

CIRA establece la responsabilidad del registrante a la hora de asegurar que el nombre de dominio elegido y la forma en que es usado no infrinjan las leyes de propiedad intelectual y patentes, no difame o discrimine a persona alguna y no quiebre ninguna ley aplicable.[58] Así, dentro de un plazo de 30 días desde el momento de la presentación, CIRA podrá eliminar o suspender discrecionalmente un registro. Podrá proceder de igual manera, sin límite de tiempo en los casos en los que la información proporcionada sea incorrecta, engañosa o incompleta; no se incumpla con los términos del acuerdo o de cualquiera de las políticas de CIRA; cuando el registrante obre de manera tal que puede comprometer a CIRA; cuando mantener el dominio implique que CIRA quebrante leyes aplicables, o decisión judicial, arbitral o administrativa, entre otras causas.[59]

---

[54] CIRA, «About the board», disponible en: http://www.cira.ca/about-cira/about-the-board/ (consultada el 18 de septiembre de 2012).

[55] CIRA, «Membership», disponible en: http://www.cira.ca/membership/ (consultada el 19 de septiembre de 2012).

[56] CIRA, «Get Involved», disponible en: https://member.cira.ca/en/involved.html (consultada el 19 de septiembre de 2012).

[57] CIRA, «Framework for the administration of the .ca domain name system», disponible en: http://www.cira.ca/assets/Documents/Publications/CDNCC-report.pdf (consultada el 18 de septiembre de 2012).

[58] CIRA, «General Registration Rules. Version 3.17», disponible en: http://cira.ca/assets/Documents/Legal/Registrars/registrationrules.pdf (consultada el 19 de septiembre de 2012).

[59] CIRA, «Registrant Agreement. Version 2.0», disponible en: http://cira.ca/assets/Documents/Legal/Registrants/registrantagreement.pdf (consultada el 19 de septiembre de 2012).

IV. El modelo argentino, NIC.ar

En el caso argentino, la organización promotora se encuentra directamente en la órbita del Poder Ejecutivo, en la Secretaría Legal y Técnica de la Presidencia de la Nación, perteneciendo así al primer grupo mencionado en las secciones anteriores.[60] Si bien siempre se la ubicó en una dependencia del Poder Ejecutivo, hasta diciembre de 2011 NIC.ar dependía del Ministerio de Relaciones Exteriores y Culto.[61] Es probable que esto haya sido así en función de la participación que la Cancillería argentina tuvo en los comienzos de Internet en Argentina,[62] pero aun así el cambio levanta dudas respecto de su efectividad para llevar a cabo las tareas necesarias para que se cumplan sus funciones en forma correcta.[63]

Una de las características llamativas de NIC.ar, que no encuentra mucha correspondencia en el resto del mundo, está relacionada con el precio que hay que pagar para iniciar el trámite destinado a obtener un nombre de dominio. Básicamente, el punto es que tal precio no existe; el registro de un nombre de dominio en Argentina es gratis. Si bien esto parece ser una ventaja deseable desde el punto de vista de la accesibilidad de los mismos, esta gratuidad debería verse acompañada de una inversión por parte del Estado, permitiendo que el registro de dominios argentino se mantenga actualizado con respecto a las distintas tecnologías existentes.

Asimismo, la gratuidad del servicio generó desde sus comienzos una avalancha de registraciones de nombres de dominio que emulaban marcas famosas en manos de personas que no eran sus propietarios, quienes esperaban obtener un beneficio económico al transferir estos dominios a los legítimos

---

60 IANA, «Delegation Record for .ar», disponible en: http://www.iana.org/domains/root/db/ar.html (consultada el 19 de septiembre de 2012).

61 El cambio fue llevado a cabo por medio del Decreto 2085/2011, que modificó el organigrama del Ministerio de Relaciones Exteriores y Culto, disponible en: http://www.boletinoficial.gov.ar/DisplayPdf.aspx?s=01&f=20111212 (consultada el 19 de septiembre de 2012).

62 Amodio, J., «Proyecto Informática de Cancillería. Historia de Internet en Argentina», disponible en: http://blog.internet-argentina.net/2010/05/08-proyecto-informatica-de-cancilleria.html (consultada el 19 de septiembre de 2012).

63 «NIC.ar pasa a la órbita de la Secretaría Legal y Técnica», *La Nación,* 14 de diciembre de 2011, disponible en: http://www.lanacion.com.ar/1432632-nicar-pasa-a-la-orbita-de-la-secretaria-legal-y-tecnica (consultada el 19 de septiembre de 2012).

propietarios.[64] Esto provocó que años después, a mediados de 2009, NIC.ar fijara en la cantidad de 200 el límite de nombres de dominio en manos de un mismo registrante.[65]

Sin embargo, la consecuencia más importante parecería estar relacionada con la inversión realizada en los sistemas por parte del administrador local. El modelo argentino no está planteado, como en otros países, en la forma de un negocio. De modo que recae en el Estado la responsabilidad de mantener el sistema actualizado, preparado para futuros cambios en la tecnología. Si bien los administradores de dominio deben, como hemos dicho, tener en cuenta que prestan un servicio público para la comunidad a la que pertenecen, también deben conducir la administración con la idea de expandir Internet. Un ejemplo de esto podría verse en la falta de innovación referente a la migración del protocolo IPv4 al IPv6.[66]

En cuanto al impacto que esto podría tener en los negocios de los usuarios, existen ciertas ventajas asociadas con el uso de dominios del ccTLD que parecen perderse o al menos disminuir cuando el operador no promociona la obtención de un dominio y sus ventajas aparejadas. Entre otras podemos mencionar la construcción integral de una marca que hoy en día incluye, casi obligatoriamente, la obtención de una página web asociada; la obtención de herramientas y recursos de parte del administrador para ayudar a los registrantes a la hora de hacer funcionar su dominio, y la tendencia de los motores de búsqueda –Google, Yahoo, etc.– de mejorar el ranking de los dominios «.ar» en las búsquedas locales.[67]

Todo parece indicar que si bien a primera vista la gratuidad del sistema argentino aumenta el acceso a Internet en forma inmediata, esta debería

---

64 Rebossio, A., «Batalla por el uso de los nombres en Internet», *La Nación,* 3 de septiembre de 2000, disponible en: http://www.lanacion.com.ar/31353-batalla-por-el-uso-de-los-nombres-en-internet (consultada el 19 de septiembre de 2012).

65 «En Argentina, sólo se podrán registrar 200 dominios», *La Nación,* 20 de mayo de 2009, disponible en: http://www.lanacion.com.ar/1130300-en-argentina-solo-se-podran-registrar- 200-dominios (consultada el 19 de septiembre de 2012).

66 Torres A., «Una mudanza que no puede hacerse esperar», *La Nación,* 16 de junio de 2012, disponible en: http://www.lanacion.com.ar/1482045-una-mudanza-que-no-puede-hacerse-esperar (consultada el 19 de septiembre de 2012).

67 NIC.us, «How .us can benefit you», disponible en: http://www.about.us/benefits/ (consultada el 19 de septiembre de 2012).

estar acompañada de una inversión y actualización constante por parte del administrador, para así evitar perder porciones del mercado mundial en manos de otros ccTLDs mejor preparados. Un cambio en este aspecto parecería deseable desde el punto de vista del acceso de los usuarios locales.[68]

Según la regulación de los procesos de registración, el solicitante deberá suministrar sus datos a NIC.ar. Esta información reviste el carácter de declaración jurada, habilitando al administrador a denegar una solicitud en caso de verificar que dicha información contiene datos erróneos, falsos o desactualizados. También podrá revocar dominios que afecten derechos subjetivos de terceros, quienes deberán acreditar fundadamente su mejor derecho, disparando el proceso administrativo correspondiente. El registro no deberá ser realizado con un propósito ilegal ni violar legislación alguna. Asimismo, NIC.ar podrá realizar revocaciones de dominio ante el pedido por medio de orden judicial.[69]

V. Conclusiones y recomendaciones

Los nombres de dominio técnicamente sólo son sucesiones de caracteres (letras, dígitos y guión, en el estándar original). Sin embargo, los nombres de dominio se encuentran «asociados» con siglas o con palabras que tienen algún significado. Es por ello que algunos nombres de dominio son considerados de alto valor comercial, al identificar marcas comerciales o palabras que identifican servicios, negocios, entidades comerciales, etc. La especulación con el valor de los nombres de dominio ha abierto mercados dinámicos y de muy alto valor comercial.

Pero además del valor comercial, también los nombres de dominio, al estar asociados con palabras que tienen significado, pueden en sí mismo estar indicando una opinión. Si alguien registra «mmm-es-corrupto» sin duda que está dando su opinión sobre «mmm» y está indicando donde pueden encontrarse, por ejemplo, más opiniones similares.

---

68 En este sentido, en los últimos meses se han anunciado cambios en varios aspectos del registro de dominios, disponible en: http://www.punto.ar/novedades/continuan-los-cambios-en-nic-argentina.php (consultada el 19 de septiembre de 2012).

69 Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, Registración de Nombres de Dominio en Internet, Resolución 654/2009, 17 de noviembre de 2009, disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/160000-164999/160861/norma.htm (consultada el 19 de septiembre de 2012).

En consecuencia, si consideramos que el valor expresivo del nombre de dominio mismo (y no solamente del contenido del recurso de Internet identificado por el nombre) es una forma de expresión y opinión, todo lo concerniente al registro o no renovación de los nombres de dominio debería someterse a los tests que protegen estos derechos fundamentales. Si conectamos la idea que el nombre de dominio en sí mismo puede ser una expresión u opinión de interés público, o que puede tener que ver con alguna crítica política a los gobiernos de turno, el diseño institucional de quienes administran los ccTLDs aparece como relevante: a mayor dominación gubernamental, mayor suspicacia respecto de razones que puedan tener que ver con la negativa de registrar o renovar dominios que puedan tener relación con una crítica al gobierno.

El caso de Argentina ejemplifica esta preocupación. En los últimos meses se han registrado ciertas irregularidades en lo referente a las registros de dominios. NIC.ar ha denegado, al menos en una primera instancia, el registro de nombres de dominio relacionados con temas políticos. Nombres de dominio relacionados con la presidente del país, Cristina Fernández de Kirchner o con la agrupación oficialista «La Cámpora» han sido denegados o se ha pedido una ampliación de la información tendiente a esclarecer la validez de la solicitud. La sola inclusión del nombre propio «Cristina» generó esta respuesta por parte del organismo, invirtiendo la lógica del proceso de registro sólo por tratarse del nombre de la presidenta.[70]

De acuerdo a los estándares internacionales que protegen la libertad de expresión, es importante destacar que la Relatoría Especial para la Libertad de Expresión (RELE) de la Comisión Interamericana de Derechos Humanos

70 «El Gobierno rechaza y se apropia de dominios de Internet con nombres K», *Perfil*, 5 de septiembre de 2012, disponible en: http://www.perfil.com/contenidos/2012/09/05/noticia_0024.html (consultada el 19 de septiembre de 2012). A mayor abundamiento, y de acuerdo a lo que surge de la respuesta del 26 de septiembre de 2012 del Director Nacional del Registro de Direcciones de Internet al pedido de acceso a la información pública efectuado por la Asociación por los Derechos Civiles (ADC) y por la Fundación Vía Libre, existen nombres de dominio cuya registración ha sido negada que, sin perjuicio de que pudieran existir razones formales que desconocemos, resultan al menos sopechosas. Entre ellos se destacan: Reclamoalgobierno.com.ar, Mireclamoalgobierno.com.ar, Lapresidentamiente.com.ar, Noticiasdecristina.com.ar, Videosdecristina.com.ar, Elgobiernomiente.com.ar, Cristinanotequiero.com.ar, defendeacristina.com.ar, Cfkblue.com.ar, Cfkmiente.com.ar, Boudumiente.com.ar, Cfktv.com.ar, Kirchnerismopasion.com.ar.

(CIDH) de la Organización de los Estados Americanos (OEA) considera que las expresiones de contenido político son las que merecen el nivel más alto de protección.

En palabras de la Relatoría:[71]

> «33. Si bien todas las formas de expresión están, en principio, protegidas por la libertad consagrada en el artículo 13 de la Convención Americana, existen ciertos tipos de discurso que reciben una protección especial, por su importancia para el ejercicio de los demás derechos humanos o para la consolidación, funcionamiento y preservación de la democracia. En la jurisprudencia interamericana, tales modos de discurso especialmente protegidos son los tres siguientes: (a) el discurso político y sobre asuntos de interés público; (b) el discurso sobre funcionarios públicos en ejercicio de sus funciones y sobre candidatos a ocupar cargos públicos; y (c) el discurso que configura un elemento de la identidad o la dignidad personales de quien se expresa».

Y sigue explicando la Relatoría que

> «36. (…) las expresiones, informaciones y opiniones atinentes a asuntos de interés público, al Estado y sus instituciones, gozan de mayor protección bajo la Convención Americana, lo cual implica que el Estado debe abstenerse con mayor rigor de establecer limitaciones a estas formas de expresión, y que las entidades y funcionarios que conforman el Estado, así como quienes aspiran a ocupar cargos públicos, en razón de la naturaleza pública de las funciones que cumplen, deben tener un mayor umbral de tolerancia ante la crítica.[72] En una sociedad democrática, dada la importancia del control de la gestión pública a través de la opinión, hay un margen reducido a cualquier restricción del debate político o de cuestiones de interés público».[73]

---

[71] Ver Informe Anual de la Relatoría Especial para la Libertad de Expresión, 2009, disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=794&lID=2 (consultada el 28 de noviembre de 2012).

[72] Corte IDH, *Caso Palamara Iribarne Vs. Chile*. Sentencia de 22 de noviembre de 2005, Serie C, Nº 135, párr. 83; Corte IDH, *Caso Herrera Ulloa Vs. Costa Rica*, Sentencia de 2 de julio de 2004, Serie C, Nº 107, párr. 125; CIDH, Alegatos ante la Corte Interamericana en el caso *Herrera Ulloa Vs. Costa Rica*, transcritos en: Corte IDH, *Caso Herrera Ulloa Vs. Costa Rica*, Sentencia de 2 de julio de 2004, Serie C, Nº 107, párr. 101.2.c.

[73] Corte IDH, *Caso Herrera Ulloa Vs. Costa Rica*, Sentencia de 2 de julio de 2004, Serie C, Nº 107, párr. 127; Corte IDH, *Caso Ivcher Bronstein Vs. Perú*, Sentencia de 6 de febrero de 2001, Serie C, Nº 74, párr. 155; CIDH, Informe Anual 1994, Capítulo V: Informe sobre la Compatibilidad entre las Leyes de Desacato y la Convención Americana sobre Derechos Humanos, Título III, OEA/Ser. L/V/II.88, doc. 9 rev. 17 de febrero de 1995.

También el Comentario General No.34 al art. 19 del Pacto Internacional de Derechos Civiles y Políticos, es importante de ser destacado, máxime, cuando hemos sostenido que el nombre de dominio puede, en muchos casos, ser en sí mismo una opinión. El Comité de Derechos Humanos, al interpretar el mencionado artículo sostuvo:

> «9. El párrafo 1 del artículo 19 exige que se proteja el derecho a no ser molestado a causa de las opiniones. Se trata de un derecho respecto del cual el Pacto no autoriza excepción ni restricción alguna. La libertad de opinión abarca el derecho a cambiar de opinión en el momento y por el motivo que la persona elija libremente. Nadie puede ver conculcados los derechos que le reconoce el Pacto en razón de las opiniones que haya expresado o le sean atribuidas o supuestas. Quedan protegidas todas las formas de opinión, como las de índole política, científica, histórica, moral o religiosa. Es incompatible con el párrafo 1 calificar de delito la expresión de una opinión.[74] El acoso, la intimidación o la estigmatización de una persona, incluida su detención, prisión preventiva, enjuiciamiento o reclusión, en razón de sus opiniones, constituyen una infracción del párrafo 1 del artículo 19».[75]

Finalmente, cualquier negativa a registrar nombres de dominio que pudiera estar vinculada con su contenido, puede ser considerada como un caso de censura previa prohibida expresamente en el sistema interamericano de protección de los derechos humanos. Es importante destacar que la Corte Interamericana de Derechos Humanos ha decidido que las limitaciones a la libertad de expresión no pueden constituir mecanismos de censura previa directa o indirecta.[76]

Por las razones aquí expuestas se sugiere:

---

[74] Véase la comunicación Nº 550/93, *Faurisson c. Francia*, dictamen aprobado el 8 de noviembre de 1996.

[75] Véanse las comunicaciones Nº 157/1983, *Mpaka-Nsusu c. el Zaire*, dictamen aprobado el 26 de marzo de 1986, y Nº 414/1990, *Mika Miha c. Guinea Ecuatorial*, dictamen aprobado el 8 de julio de 1994.

[76] Corte IDH, *Caso Kimel Vs. Argentina,* Sentencia de 2 de mayo de 2008, Serie C, Nº 177, párr. 54; Corte IDH, *Caso Palamara Iribarne Vs. Chile*, Sentencia de 22 de noviembre de 2005, Serie C, Nº 135, párr. 79; Corte IDH, *Caso Herrera Ulloa Vs. Costa Rica*, Sentencia de 2 de julio de 2004, Serie C, Nº 107, párr. 120.

• Los Estados deberían contar con administradores de registro y renovación de dominios que resulten independientes de cualquier tipo de injerencia del gobierno. Para ello, los modelos aquí reseñados que cuentan con administradores integrados por múltiples sectores puede ser un modelo a seguir.

• En caso que se opte por tener el administrador de registro y renovación de dominios en el ámbito de alguna oficina del Estado, se debería garantizar un diseño institucional que se encuentre blindado a las injerencias del gobierno. Para ello es fundamental dotar a los administradores de estabilidad y que su remoción tenga procesos especiales que impidan decisiones arbitrarias.

• En todos los casos, los administradores de registro y renovación de dominio deben tener en cuenta los estándares internacionales que garantizan el ejercicio de los derechos de opinión y expresión.

Internet y derechos humanos
Aportes para la discusión en América Latina

El Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) fue creado en el año 2009 dentro del ámbito de la Facultad de Derecho de la Universidad de Palermo con el objetivo de realizar estudios e investigaciones que se constituyan como herramientas útiles para periodistas, instituciones gubernamentales, sectores privados y de la sociedad civil dedicados a la defensa y promoción de estos derechos, especialmente en América Latina.

La creación del CELE responde a la necesidad de construir espacios de debate dedicados a reflexionar sobre la importancia, los contenidos y los límites de estos derechos en la región. Para esto, el centro se propone dialogar y trabajar en conjunto con otras unidades académicas del país y de Latinoamérica.

En este marco, los objetivos específicos del CELE son:

- Desarrollar estudios y guías de recomendaciones que tengan impacto en las políticas públicas vinculadas con el acceso a la información y a la libertad de expresión.
- Fomentar junto con distintas unidades académicas la profundización de estudios en cuestiones vinculadas con estos derechos.
- Contribuir a la generación de conciencia sobre la importancia de estos derechos en sociedades democráticas, fundamentalmente en las nuevas generaciones.

Esta publicación se realiza en el marco de un proyecto auspiciado por Global Partners Digital.







Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información
Mario Bravo 1050, 7º P. (C1175ABT) Buenos Aires | Tel.: (54 11) 5199-4500 int. 1213
www.palermo.edu/cele